ADVANCES IN MATHEMATICS 36, 1–107 (1980)

Composition of Oriented Binary Quadratic Form-Classes over Commutative Rings

JACOB TOWBER

Department of Mathematics, DePaul University, Chicago, Illinois 60614

Communicated by André Weil

INTRODUCTION

Let $G'(\delta)$ denote the set of all equivalence classes, under proper equivalence, of binary quadratic forms over $\mathbb{Z}$ of discriminant δ, and let $G(\delta)$ denote the subset of all primitive such form-classes. (It will be recalled that a binary quadratic form $ax^2 + bxy + cy^2$ with integral coefficients is called *primitive* if a, b, c have g.c.d. 1, and is called "properly equivalent" to any form obtained from it by a linear transformation with integral coefficients and determinant $+1$.)

Lagrange's theory of equivalence and reduction of quadratic forms over $\mathbb{Z}$ (1773) showed $G'(\delta)$ to be a finite set, whence $G(\delta)$ is finite; later, Gauss (1801), by a truly marvelous construction, defined on $G(\delta)$ a binary operation he called "composition," and verified that under this operation $G(\delta)$ is an Abelian group.

Two alternative ways (in addition to Gauss' original method) of constructing these composition groups were developed in the nineteenth century:

(a) the method of "united forms," due to Dirichlet and Dedekind ([17; 18, Suppl. X, Sects. 145–149]; for a modern exposition, cf. [14, Chap. IX]).

(b) an approach, due to Dedekind, based on establishing a bijection between $G(\delta)$ and the group of "narrow ideal classes" over a sultable order in $Q(\delta^{1/2})$ ([18, Suppl. X, pp. 468, 469, 488–497]; for a modern exposition, see [5, Chap. 2, Sects. 7.2, 7.4, 7.5] or [13, Chaps. 12, 13]; further references are cited at the beginning of [10]).

A number of recent papers have been concerned with the problem of generalizing this composition construction, so important in the classical theory of binary quadratic forms over $\mathbb{Z}$, to some larger class of commutative rings. This idea seems to have occurred independently to Lubelski [28], Butts and D. Estes in collaboration [9], and Kaplansky [25] (in order of publication); [28, 9] generalize the classical "united forms" method, while [25] (a study of which, together with [3], stimulated the present author to become interested in the problem of composition) generalizes Dedekind's approach via multiplication of narrow ideal-classes. The most recent paper on the subject, by Butts and Dulin [8], is based on Gauss' original approach, and obtains an extension to all rings R which satisfy the three following conditions:

0001-8708/80/040001-107$05.00/0

(BD1) R is an integral domain of characteristic $\neq 2$.

(BD2) All finitely generated projective R-modules are free.

(BD3) If x and y are in R and $x^2 \equiv y^2 \pmod{4R}$, then $x \equiv y \pmod{2R}$.

In a conversation, the present author was informed by Dullin that (BD2) may be weakened, without affecting the results or arguments in [8], to:

(BD2′) If P is an R-module with $P \oplus R^2 \approx R^4$, then $P \approx R^2$.

With this modification, the class of rings R treated in [8], i.e., those satisfying (BD1), (BD2′), (BD3), contains the rings treated by all earlier papers, the notions of composition in [8] and in each earlier paper coinciding where the latter is defined.

The purpose of the present paper is to obtain a composition construction valid over any commutative ring R with unity, subject only to the restriction that 2 is not a zero-divisor on R. One price that must apparently be paid for this degree of generality is a modification (which the author hopes may itself be of some interest) of the concept "binary quadratic form." Instead of "numerical" binary quadratic forms $ax^2 + bxy + cy^2$ over R (a, b, c in R), the objects which will here be "composed" are "oriented binary quadratic forms" over R, i.e., ordered triples (P, ϵ, q) with P an R-module such that $\Lambda^2 P$ is free over R on the "orientation" ϵ and q: $P \to R$ an R-quadratic map, i.e., such that

(1) $P \otimes P \to R$, $(p_1, p_2) \mapsto q(p_1 + p_2) - q(p_1) - q(p_2)$ is R-bilinear.

(2) $q(rp) = r^2 q(p)$ (r in R, p in P).

The numerical form-classes may in a natural way be considered as forming a subcollection of the oriented form-classes; the composite of two numerical form-classes is an oriented form-class which, in general, is not of numerical type; thus, it is only for the special class of rings for which the composite of two numerical forms is again numerical that the use of "oriented" form-classes may be avoided. This special class of rings is (as will be shown in a later paper) precisely the class of all rings R such that

(a) 2 *is not a zero-divisor on* R.

(b) *If* P *is* R*-orientable* (*cf. Definition* 1.6 *below*) *and* $P \oplus R^2 \approx R^4$, *then* $P \approx R^2$.

In this sense, Butts and Dulin have obtained (ϵ less than) the best possible result for composition (in the sense of the present paper) of *numerical* form-classes, as will be seen by comparing the preceding two conditions with the conditions (BD1), (BD2′), (BD3) listed above. It should also be mentioned that Theorem 4.5 of the present paper implies that the composition defined by the Butts–Dulin construction coincides where defined with the present one (the same being true a fortiori for all earlier constructions); however, for the class of rings considered by Butts and Dulin, the group of numerical form-classes they obtain is, in general, a proper subgroup of the group of oriented form-classes obtained in the present paper. For the ring $\mathbb{Z}$, the groups obtained in the present paper coincide with those of Gauss

(except that they include negative definite form-classes; cf. remarks at the end of Section 2).

Another new phenomenon that must be dealt with for the larger class of rings studied here is this: In addition to the familiar discriminant, which is an invariant of oriented binary quadratic forms under the suitable isomorphism concept "proper equivalence" (and is $b^2 - 4ac$ for a numerical form $ax^2 + bxy + cy^2$), it becomes necessary to also take into account what seems to be a new invariant: the "parity" of an oriented binary quadratic form, which is an element of $R/2R$ (and is $b + 2R$ for a numerical form $ax^2 + bxy + cy^2$). For the ring $\mathbb{Z}$ and indeed for the large class of rings studied by Butts and Dulin, the parity is completely determined once the discriminant is known, which perhaps accounts for its nonappearance in earlier investigations (it will readily be seen that this is the import of condition (BD3) listed above); this is no longer true for the class of rings presently to be studied. It turns out to be necessary to collect together all "primitive" oriented binary quadratic form-classes over R of given discriminant δ *and* given parity π, and indeed one does then obtain a collection $PC_R(\delta, \pi)$ upon which it is possible to induce a group structure, in a manner which is functorial in R and yields, when $R = \mathbb{Z}$, groups isomorphic to those obtained by Gauss. (It may be of interest to note that the parity may more generally be defined for oriented n-ary quadratic forms if n is even; for a *numerical* n-ary form $q(x) = \sum a_{ij}x_ix_j$ over R one obtains the parity by considering the associated symmetric bilinear form

$$B_q(x, y) = q(x + y) - q(x) - q(y)$$

over R, reducing mod 2 to obtain the associated symmetric bilinear form $\bar{B}_q$ over $R/2R$, and then taking the Pfaffien of $\bar{B}_q$ considered instead as an alternating bilinear form over $R/2R$; this is an invariant under proper equivalence.)

Section 1 of the present paper is mainly devoted to defining the notions needed merely to obtain the *set* $PC_R(\delta, \pi)$ underlying the group *operation* "composition" which will be our main object of study in later sections. Thus, the key definitions in this section are "oriented binary quadratic form-class" (Definition 1.9) and "primitive," "discriminant," "parity" (Definition 1.13). The definitions of the "discriminant" and "parity" of an oriented binary quadratic form are based on a construction (cf. Theorem 1.8) which exhibits in a quite explicit way the sense in which the two competing interpretations of "quadratic form on a module E over R"—map $E \to R$ satisfying conditions (1) and (2) above vs symmetric R-bilinear map $E \otimes E \to R$—are in fact *dual concepts*.

Section 2 is devoted to an exposition of Gauss' original composition construction, and to the derivation of two theorems (which will be needed further on), Theorems 2.5 and 2.6, concerning the Butts–Estes–Dulin generalization of Gauss' composition; this section concludes with a historical note.

The two final sections, Sections 3 and 4, are devoted to the construction of the group operation "composition" on $PC_R(\delta, \pi)$; the construction given in the

present paper differs from the three classical constructions, and may be regarded as a combination of Gauss' original approach and Dedekind's construction via "narrow ideal classes." One technical difference between the present construction and earlier ones should perhaps be noted: Composition is here also defined for *forms* (Definition 4.1), not merely for *form-classes*; this new feature is indispensable in the proofs of Theorems 4.10 and 4.11, where the existence of a composite is deduced from its existence in every localization. This property of the present construction (of yielding an operation on forms, coherently associative in the sense of [29]) also means that it extends without difficulty to sheaves of binary quadratic forms over ringed spaces.

Section 4 is devoted to studying the basic properties of the composition operation thus defined. Theorems 4.5 and 4.6 establish the connection between this composition and the Gaussian composition discussed in Section 2; this connection is exploited to prove the two main criteria for existence of a composite of two forms, namely Theorems 4.8 and 4.11. The remainder of Section 4 is devoted to the verification that $PC_R(\delta, \pi)$ is an Abelian group; a rapid summary of the results used in this verification will be found in Theorem 4.21.

This introduction is perhaps best concluded by acknowledging the author's grateful indebtedness (both as the source of many of the references given in this paper, and as a rapid introduction to the methods in the theory of composition) to Dickson's section on composition (Vol. III, Chap. III) in his scholarly labor of love [15], where the entire literature on the subject of composition prior to about 1920 is exhaustively discussed and summarized. The author also wishes to thank Professor André Weil for his encouragement and help in revising an earlier, unpublishably long version of the present paper; in particular, the definition of "parity" in Definition 1.12 below is Weil's, and replaces a clumsier (but equivalent) formulation in the earlier version.

As in all work on the subject, the debt to Gauss is perhaps too great to require mention.[1]

1. Basic Notions

1.1. *Preliminaries*

Throughout this paper, "ring" will mean commutative ring with unity, and all modules and ring-homomorphisms will be understood to be unitary. E being a module over the ring R, the usual notation

$$\Lambda E = \bigoplus_{n \geqslant 0} \Lambda^n E, \qquad E^* = \mathrm{Hom}_R(E, R)$$

[1] *Note added in proof.* Subsequent to the time this article was accepted, the author has become aware of still another approach to the construction of composition groups due to M. Kneser. Kneser's construction (not yet submitted for publication) utilizes in an elegant fashion the Clifford algebras of the forms to be composed; the relation between the composition groups he obtains, and those constructed below, is not clear at the present moment.

will be used to denote the exterior algebra on E and the module dual to E; we shall also write ${\Lambda_R}^n E$ and E_R^* when this more specific notation is required. R^n will denote the R-module whose elements are ordered n-tuples of elements of R. We shall adopt the convention that maps are written to the left of the elements on which they operate, and accordingly that the composite $f \circ g$ of two maps involves first mapping by g and then by f. Adopting this convention makes it more convenient, in the study of quadratic maps just as in the study of linear maps, to also adopt the convention that elements of R^n will be written as *columns*, or in the form ${}^t(r_1, \ldots, r_n)$. [When m and n are integers, $\binom{m}{n}$ is never in this paper to be interpreted as a binomial coefficient, but always as an element of $\mathbb{Z}^2$.]

By a *numerical n-ary Lagrangian quadratic form* over the ring R will be meant a map q, determined by $n(n+1)/2$ elements a_{ij} $(1 \leqslant i \leqslant j \leqslant n)$ of R, of the form

$$q\colon R^n \to R,\ {}^t(x_1, \ldots, x_n) \mapsto \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j\,. \tag{1}$$

Fortunately, it is not essential to distinguish between the *map* q and the *polynomial* $\sum a_{ij} x_i x_j$; the former determines the latter uniquely, since $a_{11} = q({}^t(1, 0, \ldots, 0))$, $a_{12} = q({}^t(1, \ , 0, \ldots)) - q({}^t(1, 0, 0, \ldots)) - q({}^t(0, 1, 0, \ldots))$, etc. (This no longer holds for homogeneous polynomials of degree exceeding 2; e.g., x^2y and xy^2 represent the same map over Z_2.)

Let E be a module over the ring R. It is well known that there are two senses in which we may understand the concept "quadratic form on E"; these are given in the two following definitions. These correspond to the two conventions which may be found in the literature on the theory of quadratic forms over $\mathbb{Z}$: that of Gauss, for which the coefficients a_{ij} In 1) with $i \neq j$ are required to be even, and that of Lagrange, for which this restriction is not made.

DEFINITION 1.1. Let E be a module over the ring R. By a *Gaussian* quadratic form on E over R will be meant a symmetric R-bilinear form on E, i.e., an R-homomorphism

$$B\colon E \otimes_R E \to R$$

such that

$$B(e_1 \otimes e_2) = B(e_2 \otimes e_1) \qquad (\text{all } e_1 \text{ and } e_2 \text{ in } E).$$

DEFINITION 1.2. Let E be a module over the ring R. By a *Lagrangian* quadratic form on E over R will be meant a map $q\colon E \to R$ which satisfies the following two requirements:

(i) $q(re) = r^2 g(e)$ for all r in R and e in E.

(ii) The map

$$E \otimes E \to R,\ (e_1, e_2) \mapsto q(e_1 + e_2) - q(e_1) - q(e_2)$$

is R-bilinear.

DEFINITION 1.3. Let E be a module over the ring R. We denote by $GQ_R(E)$ and $LQ_R(E)$ the R-modules formed by the set of all Gaussian quadratic forms on E over R and the set of all Lagrangian such forms, respectively. If B is a Gaussian quadratic form on E over R, then

$$E \to R,\ e \mapsto B(e \otimes e)$$

is a Lagrangian quadratic form on E over R, which we denote by q_B. If q is a Lagrangian quadratic form on E over R, then there is an associated Gaussian quadratic form on E over R, which we denote by B_q, defined by

$$B_q : E \otimes_R E \to R,\ e_1 \otimes e_2 \mapsto q(e_1 + e_2) - q(e_1) - q(e_2). \tag{2}$$

(When it makes things more readable, we shall write $B_q(e_1, e_2)$ instead of $B_q(e_1 \otimes e_2)$.)

We shall often abbreviate "Lagrangian" to "L" and "Gaussian" to "G." These two interpretations of the concept "quadratic form" differ appreciably, especially if $1_R + 1_R$ is a zero-divisor in R. One connection between them is furnished by the R-homomorphisms

$$GQ_R(E) \to LQ_R(E), \qquad B \mapsto q_B, \tag{3}$$

and

$$LQ_R(E) \to GQ_R(E), \qquad q \mapsto B_q, \tag{4}$$

which are not quite inverse: We have

$$B_{q_B} = 2B, \qquad q_{B_q} = 2q.$$

On another level, *the relation between these two concepts of quadratic form is that of duality*, in the sense of Proposition 1.3 below.

If q is a Lagrangian quadratic form on E over R, the identity

$$q\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_i q(e_i) r_i^2 + \sum_{i<j} B_q(e_i \otimes e_j)\, r_i r_j \tag{5}$$

(where all r_i are in R and all e_i in E) is readily proved by induction on n. (It suffices to prove it when all $r_i = 1$.) Thus, if E is free over R on $\{e_1, \ldots, e_n\}$, then a map $q\colon E \to R$ is an L-quadratic form on E over R if and only if there exist

$$a_{ij} \qquad (1 \leqslant 1 \leqslant j \leqslant n)$$

in R such that

$$q\left(\sum x_i e_i\right) = \sum_{i \leqslant j} a_{ij} x_i x_j \qquad \text{(all } x_i \text{ in } R\text{)}. \tag{6}$$

The associated G · quadratic form B_q on E over R is then given by

$$B_q\left(\sum x_i e_i\,,\,\sum y_j e_j\right) = \sum_i 2a_{ii}x_i y_i + \sum_{i<j} a_{ij}(x_i y_j + x_j y_i),$$

while the a_{ij}, which are uniquely determined by (6), are given by

$$a_{ii} = q(e_i),\ a_{ij} = B_q(e_i \otimes e_j) \qquad \text{if} \quad i<j.$$

In particular, the L-quadratic forms on R^n over R are exactly the numerical n-ary L-quadratic forms over R.

Dually, if E is free over R on $\{e_1,\ldots,e_n\}$, then B is a G-quadratic form on E over R if and only if there exists a symmetric $n \times n$ matrix (b_{ij}) over R such that B is the R-homomorphism $E \otimes_R E \to R$ given by

$$B\left(\left(\sum x_i e_i\right) \otimes \left(\sum y_j e_j\right)\right) = \sum_i \sum_j b_{ij}x_i y_j\,, \tag{6a}$$

and then the b_{ij} are uniquely defined by (6a) [namely, $b_{ij} = B(e_i \otimes e_j)$] and the associated L-quadratic form q_B on E over R is given by

$$q_B\left(\sum x_i e_i\right) = \sum_i b_{ii}x_i^2 + \sum_{i<j} 2b_{ij}x_i x_j\,.$$

An R-homomorphism $T\colon E' \to E$ induces R-homomorphisms

$$LQ_R(T)\colon LQ_R(E) \to LQ_R(E'), \qquad q \to q \circ T,$$

and

$$GQ_R(T)\colon GQ_R(E) \to GQ_R(E'), \qquad B \to B \circ (T \otimes T),$$

so LQ_R and GQ_R are contravariant functors from the category of R-modules into itself.

1.2. *Further Preliminaries: Change of Rings*

A ring will be called *quasi-local* if it has a unique maximal ideal; a quasi-local ring is not required to be Noetherian. The proofs in this paper continually appeal to methods involving reduction to the quasi-local case; thus care will be taken, with each new concept that is defined, to observe its behavior under localization, or more generally under change of rings. In this connection, the following notation will be adopted for the remainder of the present paper.

Let $f\colon R \to S$ be a ring-homomorphism. Any S-module E may be given the structure of an R-module by defining

$$re = f(r)e \qquad (r \text{ in } R,\ e \text{ in } E) \tag{7}$$

and we shall denote this R-module by ${}_fE$. Thus, $E \to {}_fE$ is a covariant functor from the category of S-modules to that of R-modules.

f also furnishes us with a covariant functor from the category of R-modules to that of S-modules; namely, if E is an R-module, then $E \otimes_R {}_fS$ may in a natural way be given the structure of an S-module, which we denote by E_f, while if $\alpha: E \to E'$ is an R-homomorphism we denote by α_f the S-homorphism

$$\alpha \otimes_R \mathrm{Id}_S : E_f \to F_f .$$

If e is an element of the R-module E, we denote by e_f the element $e \otimes I_S$ in E_f; note that the set of these generates E_f over S. (Like the $\otimes$ notation, this notation can lead to ambiguity if e is being considered as an element of several modules simultaneously.)

If E is projective; free, or finitely generated over R, E_f has the same property over S. $(\oplus_{i\in I} E_i)_f$ is naturally isomorphic to $\oplus_{i\in I} (E_i)_f$ (the E_i being R-modules). Recall that an f-homomorphism is a map α from an R-module E to an S-module F satisfying $\alpha(re) = f(r)\,\alpha(e)$ (r in R, e in E); then the f-homomorphism

$$E \to E_f , \; e \mapsto e_f$$

is uniquely determined to within isomorphism of E_f by the property of being an initial object in the category of all f-homomorphisms with domain E. Thus, every f-homomorphism $\alpha: E \to E'$ (E and E-module, E' and S-module), i.e., every R-homomorphism $E \to {}_fE'$, induces an S-homomorphism

$$\alpha: E_f \to E', \; e \otimes s \mapsto s\alpha(e) \qquad (e \text{ in } E, \; s \text{ in } S)$$

(the functor $E' \mapsto {}_fE'$ thus being adjoint to the functor $E \mapsto E_f$).

If Σ is an R-algebra, then Σ_f is in a natural way an S-algebra, associative (or commutative) if Σ is. If Σ is associative and E is a Σ-module, then E_f is in a natural way a Σ_f-module; if also Σ is commutative and ϕ is the ring-homomorphism

$$\Sigma \to \Sigma_f , \; \sigma \mapsto \sigma_f$$

then there is a natural Σ_f-isomorphism

$$E_\phi \approx E_f , \; e_\phi \mapsto e_f ,$$

i.e.,

$$E \otimes_\Sigma (\Sigma \otimes\!\!< {}_fS) \approx E \otimes\!\!< {}_fS$$

obtained from the natural Σ-isomorphism $E \otimes_\Sigma \Sigma \approx E$.

In the special case of these change-of-rings constructions in which P is a prime ideal of R and f is the canonical map $R \to R_P$, we shall, as is customary, write E_P, α_P, e_P instead of E_f, α_f, e_f, with similar modifications for all change-

of-rings constructions defined later in this paper (e.g., $q_{(P)}$ for $q_{(f)}$ in Definition 1.4, $\epsilon_{(P)}$ for $\epsilon_{(f)}$ in Definition 1.5).

f also transforms L- or G-quadratic forms over R into forms over S, in accordance with the following definition.

DEFINITION 1.4. Let $f\colon R \to S$ be a ring-homomorphism, E and R-module, and let q and B denote, respectively, an L- and a G-quadratic form on E over R. We define $B_{(f)}$ to be the unique G-quadratic form on E_f over S satisfying

$$B_{(f)}(e_f \otimes e'_f) = f(B(e \otimes e')) \qquad \text{(for all } e \text{ and } e' \text{ in } E) \tag{8}$$

and we define $q_{(f)}$ to be the unique L-quadratic form on E_f over S satisfying

$$q_{(f)}(e_f) = f(q(e)) \qquad \text{(for all } e \text{ in } E). \tag{9}$$

The L form thus derived from q and f is denoted by $q_{(f)}$ to distinguish it from the element q_f in the S-module $(LQ_R(E))_f$, and similarly for the notation $B_{(f)}$. The proof that there exists a unique G form $B_{(f)}$ satisfying (8) is a straightforward exercise in tensor products; the proof of the corresponding statement for $q_{(f)}$ is a bit less obvious, and may be found in [6], Proposition 3, p. 57].

PROPOSITION 1.1. *Let E_1, E_2 be R-modules; then there are natural R-isomorphisms*

$$LQ_R(E_1 \oplus E_2) \approx LQ_R(E_1) \oplus LQ_R(E_2) \oplus (E_1 \otimes_R E_2)^*,$$
$$GQ_R(E_1 \oplus E_2) \approx GQ_R(E_1) \oplus GQ_R(E_2) \oplus (E_1 \otimes_R E_2)^*.$$

COROLLARY. *If E is a finitely generated projective R-module, so are $LQ_R(E)$ and $GQ_R(E)$.*

PROPOSITION 1.2. *Let $f\colon R \to S$ be a ring-homomorphism, and let E and E' be R-modules; then there are natural S-isomorphisms*

(i) $(E \otimes_R E')_f \approx (E_f) \otimes_S (E'_f)$, $(e \otimes e')_f \mapsto e_f \otimes e'_f$,

(ii) $(\Lambda_R{}^n E)_f \approx \Lambda_S{}^n(E_f)$, $(e_1 \wedge \cdots \wedge e_n)_f \mapsto (e_1)_f \wedge \cdots \wedge (e_n)_f$.

Also, if E is a finitely generated projective R-module, there are natural S-isomorphisms

(iii) $(E^*_R)_f \approx (E_f)^*_S$, $(e^*)_f \mapsto (e_f \mapsto f(e^*(e)))$,

(iv) $[LQ_R(E)]_f \approx LQ_S(E_f)$, $q_f \mapsto q_{(f)}$,

(v) $[GQ_R(E)]_f \approx GQ_S(E_f)$, $B_f \mapsto B_{(f)}$.

Proof. The existence of the isomorphisms (i), (ii), and (iii) is standard. It is readily seen that there exists an S-homomorphism

$$\lambda(E): [LQ_R(E)] \otimes_R S \to LQ_S(E_f), \qquad q \otimes s \mapsto sq_{(f)} .$$

We shall now prove (iv) (omitting the proof of (v), which is precisely similar) by showing that $\lambda(E)$ is an isomorphism, under the following hypothesis: *The finitely generated free R-module F is the direct sum of two submodules E and E'.*

Using the natural R-isomorphism

$$LQ_R(F) \approx LQ_R(E) \oplus LQ_R(E') \oplus (E \otimes_R E')^*$$

of Proposition 1.1, $\lambda(F)$ may be decomposed into the direct sum of the three S-homomorphisms: $\lambda(E)$, $\lambda(E')$, and the S-isomorphism

$$((E \otimes_R E)^*)_f \approx (E_f \otimes_S E_f)^*;$$

the desired result then follows since $\lambda(F)$ is clearly an S-isomorphism.

PROPOSITION 1.3. *Let P denote a finitely generated projective R-module; then there is an R-bilinear pairing*

$$\langle\ ,\ \rangle_P : LQ_R(P) \otimes GQ_R(P^*) \to R$$

which is natural in R and in P in the senses indicated by Eqs. (14) *and* (15) *below, and which exhibits $LQ_R(P)$ and $GQ_R(P^*)$ as dual R-modules, that is, induces a natural R-isomorphism*

$$LQ_R(P) \approx (GQ_R(P^*))^*, \qquad q \mapsto (B^* \mapsto \langle q, B^* \rangle_P); \tag{10}$$

moreover, in the special case when P is free over R on $\{e_1, \ldots, e_n\}$, $\langle\ ,\ \rangle_P$ may be explicitly described as follows:

Let $\{e_1^*, \ldots, e_n^*\}$ be the dual basis for P^*. Let

$$q: P \to R, \sum x_i e_i \mapsto \sum_{i \leqslant j} a_{ij} x_i x_j \qquad (\text{all } a_{ij} \text{ in } R) \tag{11}$$

be a L-quadratic form on P over R, and let

$$B^*: \left(\sum x_i e_i^*\right) \otimes \left(\sum y_j e_j^*\right) \mapsto \sum_i \sum_j b_{ij} x_i y_j \qquad (\text{all } b_{ij} \text{ in } R,\ b_{ij} = b_{ji}) \tag{12}$$

be a G-quadratic form on P^* over R; then

$$\langle q, B^* \rangle = \sum_{i \leqslant j} a_{ij} b_{ij} . \tag{13}$$

Moreover, these properties determine $\langle\ ,\ \rangle$ uniquely.

Proof. For every R-module E, let $T(E)$ denote the R-homomorphism

$$T(E)\colon E \otimes_R E \to E \otimes_R E, \qquad e_1 \otimes e_2 \to e_1 \otimes e_2 - e_2 \otimes e_1 .$$

There are then natural R-isomorphisms

$$GQ_R(P) \approx \operatorname{Ker} T(P^*), \qquad LQ_R(P) \approx \operatorname{Coker} T(P^*).$$

(To see this, use Proposition 1.2 and localization to reduce to the case that P is R-free, where it is readily verified.) The desired pairing between

$$LQ_R(P) \approx \operatorname{Coker} T(P^*), \qquad GQ_R(P^*) \approx \operatorname{Ker} T(P)$$

then derives from the fact that $T(P)$, $T(P^*)$ are adjoint endomorphisms of the canonically dual R-modules $P \otimes_R P$ and $P^* \otimes_R P^*$.

It follows readily that if $f\colon R \to S$ is a ring-homomorphism then

$$\langle q_{(f)} , B^*_{(f)} \rangle_{P_f} = f(\langle q, B^* \rangle_P) \tag{14}$$

and that if $T\colon P \to P_1$ is an R-homomorphism of finitely generated projective R-modules, with

$$q_1 \in LQ_R(P_1),\ B^* \in GQ_R(P^*)$$

then

$$\langle LQ_R(T) q_1 , B^* \rangle_P = \langle q_1 , GQ_R(T^*) B^* \rangle_{P_1} \tag{15}$$

COROLLARY 1. *If P is a finitely generated projective R-module, there are R-isomorphisms (natural in R and P):*

$$GQ_R(P) \approx [LQ_R(P^*)]^*,\ LQ_R(P^*) \approx [GQ_R(P)]^*,\ GQ_R(P^*) \approx [LQ_R(P)]^*.$$

Proof. These follow from (10), the natural isomorphism $P \to P^{**}$, and the fact that, by Proposition 1.1, $LQ_R(P)$ and $GQ_R(P)$ are finitely generated projective R-modules.

COROLLARY 2. *Given a L-quadratic form q over R on the finitely generated projective R-module P, there exists $\alpha^* = \sum f_i \otimes q_i$ in $P^* \otimes_R P^*$ such that*

$$q(p) = \sum f_i(p)\, g_i(p) \qquad (\textit{all } p \textit{ in } P).$$

if also α in $P^* \otimes_R P^*$ has this property, then there exist f'_j, g'_j in P^* with

$$\alpha_1^* = \alpha^* + \sum_j (f'_j \otimes g'_j - g_j \otimes f'_j).$$

Proof. The map cls $\alpha^* \to q$ is exactly the isomorphism

$$\text{Coker } T(P^*) \approx LQ_R(P)$$

described in the preceding proof.

1.3. *Oriented Modules*

DEFINITION 1.5. A module P over R will be called *R-orientable of rank n* if $\Lambda^n P$ is free of rank 1 over R; a free generator ϵ of $\Lambda^n P$ will then be called an *R-orientation* of P, and we say that the ordered pair (P, ϵ) is a *rank n R-oriented R-module.* Two R-oriented R-modules (P, ϵ) and (P_1, ϵ_1) of the same rank n will be called *R-orientedly R-isomorphic* if there exists an R-isomorphism $T: P \to P_1$ such that $\Lambda^n T: \Lambda^n P \to \Lambda^n P_1$ maps ϵ into ϵ_1, and such a T will then be called an *R-oriented R-isomorphism* from (P, ϵ) to (P_1, ϵ_1). If ϵ is a rank n R-orientation of P, and $f: R \to S$ is a ring-homomorphism, we denote by $\epsilon_{(f)}$ the image of $\epsilon \otimes I_S$ under the ring-isomorphism

$$(\Lambda_R{}^n P) \otimes_R S \to \Lambda_S{}^n(P_f)$$

of Proposition 1.2(ii).

Remarks. If ϵ is a rank n R-orientation of P, the most general rank n R-orientation of P is $u\epsilon$, with u a unit of R. A free R-module F of rank n is clearly rank n R-orientable: If F is free over R on $\{e_1, \ldots, e_n\}$, then $\Lambda^n F$ is free on $e_1 \wedge \cdots \wedge e_n$; calling two free bases for F over R "equivalent" if the $n \times n$ matrix over R which transforms one into the other has determinant 1, there is an obvious one-to-one correspondence

$$\text{cls}\{e_1, \ldots, e_n\} \mapsto e_1 \wedge \cdots \wedge e_n$$

between the equivalence classes of free bases for F over R and the R-orientations of F.

If ϵ is a rank n R-orientation of P, and $f: R \to S$ is a ring-homomorphism, then $\epsilon_{(f)}$ is a rank n R-orientation of P_f, i.e., a free generator of $\Lambda_S{}^n P_f$, since $e \otimes I_S$ is a free generator of $(\Lambda_R{}^n P) \otimes_R S$. Hence, if P is a R-orientable module over R, then P_f is S-orientable. $\epsilon_{(f)}$ may be defined more concretely as follows: If

$$\epsilon = \sum_i p_{i1} \wedge \cdots \wedge p_{in} \qquad (\text{all } p_{ij} \text{ in } P),$$

then

$$\epsilon_{(f)} = \sum_i (p_{i1})_f \wedge \cdots \wedge (p_{in})_f .$$

If T is an R-oriented R-isomorphism from (P, ϵ) to (P', ϵ'), then T_f is an S-oriented S-isomorphism from $(P_f, \epsilon_{(f)})$ to $(P'_f, \epsilon'_{(f)})$.

Professor Rota has pointed out to the author that when R is a field, the R-oriented R-modules are precisely the "Cayley spaces" defined by Doubilet, Rota, and Stein, in the monograph "On the Foundations of Combinatorial Theory, IX" Studies in Applied Mathematics, Vol. LIII, pp. 185–216.

PROPOSITION 1.4 (H. Flanders). *An R-orientable R-module is finitely generated and projective over R.* (This is Theorem 3 of [21].)

COROLLARY 1. *If the R-module P is rank n R-orientable, then for every prime ideal M of R, P_M is free of rank n over R_M.*

Proof. For every prime ideal M of R, P_M is free over R_M and rank n R_M-orientable, hence is free over R_M of rank n.

COROLLARY 2. *An R-module cannot be R-orientable of two distinct ranks.*

PROPOSITION 1.5. *If P is an R-module, and $\Lambda^n P$ is free over R on the element $p_1 \wedge \cdots \wedge p_n$ (p_i in P), then P is free over R on $\{p_1, \ldots, p_n\}$.*

Proof. Let p be an element of P. If

$$p = r_1 p_1 + \cdots + r_n p_n \qquad (r_i \text{ in } R), \tag{16}$$

then the r_i are uniquely determined by

$$r_i p_1 \wedge \cdots \wedge p_n = (-1)^{i-1} p \wedge p_1 \wedge \cdots \wedge \hat{p}_i \wedge \cdots \wedge p_n \quad (1 \leqslant i \leqslant n, r_i \text{ in } R) \tag{17}$$

(where the caret over p_i indicates it is to be deleted from the wedge product). Thus, $p_1, \ldots, p_n$ are linearly independent over R.

To show that $p_1, \ldots, p_n$ generate P over R, it suffices to show that, conversely, (17) implies (16). This implication is easy to prove if P is free over R (in which case P is easily seen to be free over R on $\{p_1, \ldots, p_n\}$, from which (17) $\Rightarrow$ (16) is immediate), and follows in the general case by a localization argument (which uses Proposition 1.4).

DEFINITION 1.6. Let $T: P \to P$ be an R-endomorphism of the rank n P-orientable R-module P. Since $\Lambda^n P$ is free of rank 1 over R, there exists a unique element of R such that

$$\Lambda^n T: \Lambda^n P \to \Lambda^n P$$

is multiplication by this element on $\Lambda^n P$, and we denote this element of R by $\det_R T$, the determinant of T over R. Let g be the inclusion map $P \to P[X]$,

where X is an indeterminate over R; by $\chi_R(T)(X)$, the *characteristic polynomial* of T over R, will be meant the element

$$\det_{R[X]}(X\,\mathrm{Id}_{P_g} - T_g)$$

in $R[X]$. (Note that this makes sense, since P_β is $R[X]$-orientable by the remarks preceding Proposition 1.4.) Finally, we define $\mathrm{tr}_R T$, the *trace* of T over R, to be the negative of the coefficient of X^{n-1} in $\chi_R(T)(X)$.

Remarks. If P is a finitely generated free R-module, the notions of determinant, characteristic polynomial, and trace just defined for R-endomorphisms of P coincide with the usual ones. Also, $\det_R$, and hence χ_R and tr_R, behave well under change of rings; more precisely, under the hypotheses of Definition 1.6, and $f\colon R \to S$ being a ring-homomorphism, we have

$$\det_S T_f = f(\det_R T), \qquad \mathrm{tr}_S T_f = f(\mathrm{tr}_R T),$$

and (assuming X remains an indeterminate over S)

$$\chi_S(T_f)(X) = f_1(\chi_R(T)(X)),$$

where $f_1 : R[X] \to S[X]$ is canonically induced by f.

PROPOSITION 1.6. *If T is an R-endomorphism of a rank n R-orientable R-module, then its characteristic polynomial is monic of degree n and constant term $(-1)^n \det_R T$. The Cayley–Hamilton theorem holds, i.e.,*

$$\chi_R(T)(T) = 0.$$

Proof. By localization.

We next observe some additional structure, which will be of great use to us, associated with rank 2 oriented modules.

DEFINITION 1.7. Let (P, ϵ) be a rank 2 R-oriented R-module; then by Φ_ϵ will be meant the R-bilinear alternating form

$$\Phi_\epsilon : P \otimes_R P \to R$$

on P uniquely defined by

$$p_1 \wedge p_2 = \Phi_\epsilon(p_1 \otimes p_2)\epsilon \qquad (p_1 \text{ and } p_2 \text{ in } P).$$

By λ_ϵ will be meant the R-homomorphism

$$\lambda_\epsilon : P \to P^*, \qquad p_1 \mapsto (p_2 \mapsto \Phi_\epsilon(p_1 \otimes p_2)).$$

Remark. If P is free over R, we may pick a free basis $\{e_1, e_2\}$ such that $e_1 \wedge e_2 = \epsilon$; let (e_1^*, e_2^*) be the dual basis; then Φ_ϵ and λ_ϵ are given by the formulas

$$\Phi_\epsilon((x_1e_1 + x_2e_2) \otimes (y_1e_1 + y_2e_2)) = \begin{vmatrix} x_1, & x_2 \\ y_1, & y_2 \end{vmatrix}, \tag{18}$$

$$\lambda_\epsilon(x_1e_1 + x_2e_2) = -x_2e_1^* + x_1e_2^*. \tag{19}$$

LEMMA 1.7. *Let (P, ϵ) be a rank 2 R-oriented R-module; then:*

(i) *λ_ϵ is an R-isomorphisms.*

(ii) *If $f: R \to S$ is a ring-homomorphism, then*

$$\Phi_{(\epsilon_{(f)})}(p_f \otimes p_f') = f(\Phi_\epsilon(p \otimes p')) \qquad (\textit{for all } p, p' \textit{ in } P)$$

and the following diagram commutes:

$$\begin{array}{ccc} & & P_f \\ & {\scriptstyle (\lambda_\epsilon)_f} \swarrow & \downarrow {\scriptstyle \lambda_{(\epsilon_{(f)})}} \\ (P_R^*)_f & \longrightarrow & (P_f)_S^* \end{array}$$

where the horizontal arrow denotes the isomorphism of Proposition 1.2(iii).

(iii) *If also (P', ϵ') is a rank 2 R-oriented R-module, and T is an R-oriented R-isomorphism from (P, ϵ) to (P', ϵ'), then for all p and p' in P,*

$$\Phi_\epsilon(p \otimes p') = \Phi_{\epsilon'}(Tp \otimes Tp'), \qquad \lambda_\epsilon(p) = T^*(\lambda_{\epsilon'}(Tp)).$$

Remark. (i) occurs in Bass' study of (G-) quadratic and bilinear forms on modules [3, Proposition 4.4].

Proof of Lemma 1.7. (ii) is straightforward, and may be used to reduce by localization the proof of (i) to the special case that P is free over R, when (i) follows immediately from (19). (Note: this argument involves the use of Proposition 1.2(iii), which requires that P be finitely generated and projective; thus, Flanders' result is essential here, as in several later localization arguments.)

(iii) is straightforward.

1.4. *Oriented Quadratic Forms*

DEFINITION 1.8. By an *oriented n-ary Lagrangian quadratic form* over the ring R will be meant an ordered triple (P, ϵ, Q) with (P, ϵ) a rank n R-oriented R-module, and Q a Lagrangian quadratic form on P over R.

Let

$$\gamma = (P, \epsilon, Q), \qquad \gamma' = (P', \epsilon', Q')$$

be two such; by a proper R-equivalence from γ to γ' will be meant an R-oriented R-isomorphism T of (P, ϵ) into (P', ϵ') such that

$$Q = Q' \circ T \tag{20}$$

and if such a T exists γ and γ' will be said to be properly equivalent over R. The equivalence class of γ with respect to proper R-equivalence will be denoted by $\operatorname{cls}\gamma$; such an equivalence class will be called a *proper n-ary Lagrangian quadratic form-class over R.*

If $f\colon R \to S$ is a ring-homomorphism and $\gamma = (P, \epsilon, Q)$ is as above, we define γ_f to be $(P_f, \epsilon_{(f)}, Q_{(f)})$, which is an oriented n-ary Lagrangian quadratic form over S; $(\operatorname{cls}\gamma)_f$ is well defined by

$$(\operatorname{cls}\gamma)_f = \operatorname{cls}(\gamma_f)$$

and is a proper n-ary Lagrangian quadratic form-class over S.

Oriented n-ary Gaussian quadratic forms over R, and the various related concepts, are defined by simply replacing the word "Lagrangian" by "Gaussian" in the preceding, also replacing (20) by

$$Q = Q'(T \otimes_R T).$$

DEFINITION 1.9. Suppose $\gamma = (P, \epsilon, Q)$ is an oriented n-ary L-quadratic form over the ring R, and let $T\colon P \to P'$ be an R-isomorphism; then we define the oriented n-ary L-quadratic form $T_*\gamma = (P', T_*\epsilon, T_*Q)$ over R by

$$T_*\epsilon = A^n(T)\epsilon, \qquad T_*Q = LQ_R(T^{-1})Q.$$

The same definition is to hold with L replaced everywhere by G.

PROPOSITION 1.8. *Under the hypotheses of Definition* 1.9 (*either with L or G*), *$T_*\gamma$ is the unique form γ' such that T is a proper R-equivalence from γ to γ'.*

Proof. Obvious.

The only case that concerns us for the remainder of this paper is $n = 2$, i.e., oriented *binary* L-quadratic forms; these, and their form-classes, are the objects that get composed. Accordingly, from now on we shall usually speak simply of oriented (or numerical) L (or G) forms, *with "binary" and "quadratic" omitted and understood.*

Let us now consider in some detail numerical (binary quadratic) L forms over R in the context of Definition 1.8. A numerical L form over R is a map

$$[a, b, c]^L\colon R^2 \to R, \qquad \binom{x}{y} \mapsto ax^2 + bxy + cy^2,$$

i.e., is a L form on R^2 over R. We associate with this the oriented L form

$$\gamma[a, b, c]^L = \left(R^2, \binom{1}{0} \wedge \binom{0}{1}, [a, b, c]^L\right). \tag{21}$$

So much for the objects; now for the morphisms. Given a numerical L form $[a, b, c]^L$ over R and a 2×2 matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ over R, the map

$$R^2 \to R, \binom{x}{y} \mapsto [a, b, c]^L \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\binom{x}{y}\right)$$

is again a numerical L form, which we denote by $[a, b, c]^L \circ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. It is readily verified that

$$[a, b, c]^L \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = [a', b', c']^L$$

with

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 = [a, b, c]^L \left(\binom{\alpha}{\gamma}\right), \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = B_{[a,b,c]^L}\left(\binom{\alpha}{\gamma} \otimes \binom{\beta}{\delta}\right), \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 = [a, b, c]^L \left(\binom{\beta}{\delta}\right). \end{aligned} \tag{22}$$

Two numerical L forms $[a, b, c]^L$ and $[a', b', c']^L$ are said to be *properly equivalent* over R when there exists a matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ over R with

$$\alpha\delta - \beta\gamma = 1 \tag{23}$$

and such that

$$[a', b', c']^L = [a, b, c]^L \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

This is exactly the condition that the associated oriented L forms $\gamma[a, b, c]^L$ and $\gamma[a', b', c']^L$ be properly equivalent over R, i.e., that there exist an R-isomorphism $T: R^2 \to R^2$ such that

$$\Lambda^2 T\left(\binom{1}{0} \wedge \binom{0}{1}\right) = T\binom{1}{0} \wedge T\binom{0}{1} = \binom{1}{0} \wedge \binom{0}{1}, [a', b', c']^L = [a, b, c]^L \circ T.$$

(Note: T is then a proper equivalence over R from $\gamma[a', b', c']^L$ to $\gamma[a, b, c]^L$.) By a *proper numerical L form-class* over R will be meant the set of all numerical L forms over R properly equivalent over R to a given one. The collection of

proper L form-classes over R is richer than the collection of proper numerical L form-classes over R; by the preceding, there is an injective mapping

$$\mathrm{cls}[a, b, c]^L \to \mathrm{cls}\,\gamma[a, b, c]^L$$

from the latter collection into the former one. The image of this injection contains cls γ if and only if $\gamma = (P, \epsilon, q)$ is *free* (i.e., P is free; cf. Definition 1.10 below) in which case we say also that cls γ is free. As we shall see, it is possible that the composite of two free form-classes is not itself free; in such a situation, composition cannot be satisfactorily defined so long as we are restricted to numerical form-classes.

A numerical L form $[a, b, c]^L$ over R has the following three invariants with respect to proper equivalence over R, each of which is important for the theory of composition: Its *discriminant* $b^2 - 4ac$; its *divisor*, the ideal

$$\mathrm{div}_R[a, b, c]^L = Ra + Rb + Rc; \tag{24}$$

its *parity*, the residue class of its middle coefficient b in $R/2R$. It is classical that (22) implies

$$b'^2 - 4a'c' = (\alpha\delta - \beta\gamma)^2(b^2 - 4ac),$$

whence (23) implies $b'^2 - 4a'c' = b^2 - 4ac$; it is clear (22) implies $Ra + Rb + Rc \supseteq Ra' + Rb' + Rc'$, and we may here replace $\supseteq$ by $=$, since proper equivalence over R is a symmetrical relation; finally, (22) and (23) imply;

$$b' \equiv b(\alpha\delta + \beta\gamma) \equiv b(\alpha\delta - \beta\gamma) \equiv b \pmod{2R}.$$

DEFINITION 1.10. Let $\gamma = (P, \epsilon, q)$ be an oriented binary L-quadratic form over the ring R. We say γ is *free* if P is free over R; there then exists a free basis $\{e_1, e_2\}$ for P over R such that $e_1 \wedge e_2 = \epsilon$ and we say that such a free basis is *properly oriented*; such being the case, there then exist a, b, and c in R such that

$$q(xe_1 + ye_2) = ax^2 + bxy + cy^2 \qquad (\text{all } x \text{ and } y \text{ in } R) \tag{25}$$

and we say: γ *is represented by* $[a, b, c]^L$ *with respect to the properly oriented free basis* $\{e_1, e_2\}$, and also say γ *is associated with* $[a, b, c]^L$.

Suppose the oriented L form $\gamma = (P, \epsilon, q)$ is represented by the numerical L form $[a, b, c]^L$ with respect to the properly oriented free basis $\{e_1, e_2\}$ for P over R. If $\{e_1', e_2'\}$ is another properly oriented free basis for P over R, then

$$e_1' = \alpha e_1 + \gamma e_2, \qquad e_2' = \beta e_1 + \delta e_2$$

with α, β, γ, δ in R, $\alpha\delta - \beta\gamma = 1$; moreover, it is readily seen that then γ is represented by the numerical L form $[a, b, c]^L \circ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ with respect to the properly oriented free basis $\{e_1', e_2'\}$. Thus, all numerical L forms associated with a given

oriented L form γ are properly equivalent over R, and make up a proper numerical L form-class over R. Hence, we may unambiguously define the discriminant, parity, and divisor of a free oriented L form γ to be those of any numerical L form associated with γ. (In Definition 1.12 we shall see how to define these three invariants for oriented L forms which are not free.)

Note also that if the oriented L form γ is represented by $[a, b, c]^L$ with respect to the properly oriented basis $\{e_1, e_2\}$, then

$$R^2 \to P, \begin{pmatrix} x \\ y \end{pmatrix} \to xe_1 + ye_2$$

is a proper R-equivalence from $\gamma[a, b, c]^L$ to γ.

Suppose we are furnished with a rank 2 free R-module P and with an L form q on P over R, but *not* with any particular R-orientation for P. Associated with every free basis $\{e_1, e_2\}$ for P there is a numerical L form $[a, b, c]^L$ satisfying (25); let C denote the set of all such $[a, b, c]^L$ corresponding to all possible free bases for P. This set C is no longer a proper numerical L form-class, as was the case in the preceding paragraph, where P was furnished with an R-orientation and we restricted ourselves to free bases belonging to that orientation. Rather, it is readily seen that C is an equivalence class for the equivalence relation obtained if we replace (23) by the weaker condition.

$$\alpha\delta - \beta\gamma \text{ is a unit in } R. \tag{23a}$$

This weaker equivalence relation between forms is too gross to be suitable for the quite delicate constructions involved in composition (as will become clear for the case $R = \mathbb{Z}$ in Section 2) which explains the necessity for including an orientation as part of the structure of the forms we shall study in this paper.

By combining the bilinear pairing $\langle\ ,\ \rangle_P$ between $LQ(P)$ and $GQ(P^*)$ of Proposition 1.3 with the R-isomorphism $\lambda_c : P \approx P^*$ of Definition 1.7 and Lemma 1.7, we obtain the following bilinear pairing between $LQ(P)$ and $GQ(P)$.

DEFINITION 1.11. Let (P, ϵ) be a rank 2 R-oriented R-module; then by $\langle\ \cdot\ \rangle_{0,\epsilon}$ will be meant the R-bilinear pairing

$$LQ_R(P) \otimes GQ_R(P) \to R$$

defined by

$$\langle q, B\rangle_{P,\epsilon} = \langle q, GQ_R((\lambda_\epsilon)^{-1})B\rangle_P .$$

PROPOSITION 1.9. *Let (P, ϵ) be a rank 2 R-oriented R-module. Let P be free over R on $\{e_1, e_2\}$, with $e_1 \wedge e_2 = \epsilon$. Let (for elements a, b, c, a', b', c' in R) q and B,*

respectively, denote the L and G form on P over R given, respectively, by the formulas

$$q(x_1e_1 + x_2e_2) = ax_1^2 + bx_1x_2 + cx_2^2,$$
$$B((x_1e_1 + x_2e_2) \times (y_1e_1 + y_2e_2)) = a'x_1y_1 + b'(x_1y_2 + x_2y_1) + c'x_2y_2 .$$

Then

$$\langle q, B\rangle_{P,\epsilon} = ac' - bb' + ca'. \tag{26}$$

Remark. This "joint invariant of two quadratic forms" was well known in the classical theory of invariants; cf. for example [23], Chaps. 1, 2].

Proof of Proposition 1.9. It is immediate from (19) that

$$(\lambda_\epsilon)^{-1}(x_1e_1^* + x_2e_2^*) = x_2e_1 - x_1e_2$$

whence

$$GQ_R(\lambda_\epsilon^{-1})(B)((x_1e_1^* + x_2e_2^*) \otimes (y_1e_1^* + y_2e_2^*))$$
$$= B((x_2e_1 - x_1e_2) \otimes (y_2e_1 - y_1e_2)) = c'x_1y_1 - b'(x_1y_2 + x_2y_1) + a'x_2y_2 .$$

Applying Eq. (13) we obtain

$$\langle q, B\rangle_{P,\epsilon} = \langle q, GQ_R(\lambda_\epsilon^{-1})B\rangle_P = ac' - bb' + ca'$$

as asserted.

LEMMA 1.10. *Let (P, ϵ) be an R-oriented R-module, let*

$$q \in LQ_R(P), \qquad B \in GQ_R(P)$$

and let $f: R \to S$ be a ring-homomorphism; then

$$\langle q_{(f)}, B_{(f)}\rangle_{P_f,\epsilon_{(f)}} = f(\langle q, B\rangle_{P,\epsilon}).$$

If also $T: P \to P'$ is an R-isomorphism, then

$$\langle LQ_R(T^{-1})q, GQ_R(T^{-1})B\rangle_{P',(\Lambda^2 T)\epsilon} = \langle q, B\rangle_{P,\epsilon} .$$

Proof. Straightforward, using the definition of $\langle\ ,\ \rangle_{P,\epsilon}$ together with Lemma 1.7 and Eqs. (14) and (15) of Proposition 1.3.

DEFINITION 1.12. Let $\gamma = (P, \epsilon, q)$ be an oriented binary Lagrangian quadratic form. The *discriminant* of γ, denoted by $\delta(\gamma)$, is defined (cf. Definition 1.3) by

$$\delta(\gamma) = -\langle q, B_q\rangle_{P,\epsilon} .$$

By the divisor of γ, denoted by div γ, will be meant the ideal generated over R by $\{q(p)\colon p \text{ in } P\}$. We call γ primitive if div $\gamma = R$, and we call two such forms γ and γ' *comaximal* if

$$\text{div } \gamma + \text{div } \gamma' = R.$$

By the *parity* of γ, denoted by $\pi(\gamma)$, will be meant the element of $R/2R$ uniquely determined by the requirement that

$$B_q(p, p') \equiv \pi(\gamma)\, \Phi_\epsilon(p, p') \qquad (\text{mod } 2R)$$

hold for all p, p' in R (cf. Definition 1.7).

Remark. It is readily verified that these reduce to the earlier definitions when P is free.

LEMMA 1.11. *Let $\gamma = (P, \epsilon, q)$ be an oriented L form over the ring R, let $f\colon R \to S$ be a ring-homomorphism, and let $T\colon P \to P'$ be a proper R-equivalence from γ to another form γ'; then:*

(i) *$\gamma' = T_*\gamma$ has the same discriminant, divisor and parity as γ;*

(ii) *$\delta(\gamma_f) = f(\delta(\gamma))$, $\text{div } \gamma_f = f(\text{div } \gamma)S$ and*

$$\pi(\gamma) = r + 2R \Rightarrow \pi(\gamma_f) = f(r) + 2S.$$

Proof. Straightforward.

DEFINITION 1.13. Let Γ be a proper L form-class over R; by the discriminant $\delta(\Gamma)$, divisor div Γ, and parity $\pi(\Gamma)$ of Γ will be meant the discriminant, divisor, and parity, respectively, of any form in Γ. (This definition is unambiguous by Lemma 1.11 (i).)

PROPOSITION 1.12. *Let γ be an oriented L form over the ring R; then the ideal* div γ *is finitely generated over R, and*

$$\delta(\gamma) \in (\text{div } \gamma)^2. \tag{27}$$

Proof. Let $\gamma = (P, \epsilon, q)$. By Proposition 1.9, P is finitely generated over R, say by $\{e_1, \ldots, e_n\}$. Then div γ contains the $n(n+1)/2$ quantities:

$$q(e_i),\ B_q(e_i \otimes e_j) = q(e_i + e_j) - q(e_i) - q(e_j)$$

and the ideal generated over R by these quantities contains (hence equals) div γ because it contains $q(p)$ for all $p = r_1e_1 + \cdots + r_ne_n$ $(r_i \in R)$ in P, by (5).

Lemma 1.11(ii) enables us, by the method of localization, to reduce the proof of (27) to the case that γ is free, when it follows immediately from the obvious fact

$$b^2 - 4ac \in (Ra + Rb + Rc)^2.$$

PROPOSITION 1.13. *Let $\delta \in R$, $\pi \in R/2R$. The following four statements are equivalent:*

(i) *There exist b and c in R such that the numerical L form $[1, b, c]^L$ over R has discriminant δ and parity π.*

(ii) *There exists a primitive oriented L form over R of discriminant δ and parity π.*

(iii) *There exists an oriented L form over R of discriminant δ and parity π.*

(iv) *The map*

$$Sq\colon R/2R \to R/4R,\ r + 2R \to r^2 + 4R$$

sends π into $\delta + 4R$.

Proof. Clearly (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii).

(iii) $\Rightarrow$ (iv). Let $\gamma = (P, \epsilon, q)$ have discriminant δ and parity $\pi = r + 2R$. Let M be a maximal ideal of R. By (ii) of Lemma 1.11, $\gamma_M = (P_M, \epsilon_M, q_M)$ has discriminant δ_M and parity $r_M + 2R_M$. P_M is free over R_M; if $\{e_1, e_2\}$ is any free basis for P_M over R_M with $e_1 \wedge e_2 = \epsilon_M$, and $[a, b, c]^L$ represents q_M with respect to this free basis (a, b, and c in R_M), then $b^2 - 4ac = \delta_M$, $b + 2R_M = r_M + 2R_M$, so $b - r_M \in 2R_M$, ${b_M}^2 - {r_M}^2 \in 4R_M$, $\delta_M - {r_M}^2 \in 4R_M$. This is true for every maximal ideal M of R, so $\delta - r^2 \in 4R$, i.e., $\delta + 4R = Sq(\pi)$.

(iv) $\Rightarrow$ (i). Suppose $\pi = b + 2R$, $Sq(\pi) = \delta + 4R$; then $b^2 = \delta + 4c$ for some c in R, and $[1, b, c]^L$ is the required numerical L form.

Buttes and Estes introduce, in their study [9] of the "united forms" method of composition over commutative rings, the following condition on the ring R, which they call "Condition C":

$$x \text{ and } y \text{ in } R,\ x^2 \equiv y^2 \pmod{4R} \text{ imply } x \equiv y \pmod{2R}.$$

By the preceding proposition, we may view the significance of the Buttes–Estes condition in this way: It is equivalent to the assertion that all oriented L forms over R of given discriminant have the same parity (or again, to the assertion that all *primitive* oriented L forms over R of the same discriminant have the same parity; also, we may replace "oriented" by "numerical" in these two statements). This is the case for the ring $\mathbb{Z}$, which is why the parity plays no role independent of the discriminant in the theory of binary L quadratic forms over $\mathbb{Z}$, unlike the situation over more general rings. In fact, the Buttes–Estes condition is satisfied by any integrally closed domain, as Buttes and Estes prove [9] by the following argument: The assertion is trivial in characteristic 2; if char $R \neq 2$ and if $t = \frac{1}{4}(x^2 - y^2)$ is in R, then the element $u = \frac{1}{2}(x - y)$ of the quotient-field of R is integral over R, hence in R, since u satisfies $u(u + y) = t$.

For the sake of symmetry we introduce here the following brief sketch of

some analogous notions for Gaussian forms; these notions, however, will not be used again in the present paper.

A (binary) numerical Gaussian (quadratic) form over R is a map

$$[a, b, c]^G: R^2 \otimes_R R^2 \to R, \binom{x_1}{x_2} \otimes \binom{y_1}{y_2} \to ax_1y_1 + b(x_1y_2 + x_2y_1) + cx_2y_2$$

and has associated with it the oriented G form

$$\gamma[a, b, c]^G = \left(R^2, \binom{1}{0} \wedge \binom{0}{1}, [a, b, c]^G\right).$$

$[a, b, c]^G$ and $[a', b', c']^G$ will be called *properly equivalent* over R when there exists a 2×2 matrix $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ over R of determinant 1 such that

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = {}^tT \begin{pmatrix} a & b \\ b & c \end{pmatrix} T,$$

i.e., such that

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = [a, b, c]^G\left(\binom{\alpha}{\gamma} \otimes \binom{\alpha}{\gamma}\right),$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = [a, b, c]^G\left(\binom{\alpha}{\gamma} \otimes \binom{\beta}{\delta}\right),$$

$$c' = a\beta^2 + 2b\beta\delta + c\delta^2 = [a, b, c]^G\left(\binom{\beta}{\delta} \otimes \binom{\beta}{\delta}\right).$$

It is readily seen that this is the case if and only if $\gamma[a, b, c]^G$ and $\gamma[a', b', c']^G$ are properly equivalent over R.

We define the *determinant* of $[a, b, c]^G$ to be $\left|\begin{smallmatrix} a, & b \\ b, & c \end{smallmatrix}\right| = ac - b^2$, and its *divisor* to be $Ra + Rb + Rc$; it is readily seen that properly equivalent numerical G forms have the same determinant and divisor. We may extend these notions to an oriented G form $\gamma = (P, \epsilon, B)$ over R as follows: The *divisor* $\operatorname{div}\gamma$ is the ideal in R generated by $\{B(p_1 \otimes p_2)\colon p_1 \text{ and } p_2 \text{ in } P\}$, and (cf. [3]) the *determinant* of γ is

$$\Lambda^2 B(\epsilon \otimes \epsilon)$$

where $\Lambda^2 B$ denotes the (1-ary) G quadratic form on $\Lambda^2 P$ over R defined by

$$(\Lambda^2 B)((p_1 \wedge p_2) \otimes (q_1 \wedge q_2)) = \begin{vmatrix} B(p_1 \otimes q_1), & B(p_1 \otimes q_2) \\ B(p_2 \otimes q_1), & B(p_2 \otimes q_1) \end{vmatrix}.$$

(It is readily verified that the divisor and determinant of $\gamma[a, b, c]^G$ are those of $[a, b, c]^G$.) By the *oriented L form associated to* γ, denoted by γ_L, we mean (P, ϵ, q_B).

Let γ and γ' be oriented G forms over R. We say γ is *primitive* if $\operatorname{div}\gamma = R$, γ and γ' are *comaximal* if $\operatorname{div}\gamma + \operatorname{div}\gamma' = R$. We say γ is *properly primitive* if $\operatorname{div}\gamma_L = R$, γ and γ' are *properly comaximal* if $\operatorname{div}\gamma_L + \operatorname{div}\gamma'_L = R$; these are apparently more relevant notions than the two preceding ones for the theory of composition. A localization argument shows that $\operatorname{div}\gamma \supseteq \operatorname{div}\gamma_L$, so "properly primitive" implies "primitive," "properly comaximal" implies "comaximal" (but not conversely).

We note finally that the G form associated with $[a, b, c]^L$ is $[2a, b, 2c]^G$, while the L form associated with $[a, b, c]^G$ is $[a, 2b, c]^L$ (thus, an elementary localization argument shows the parity of the oriented L form associated with any oriented G form is 0).

2. The Gaussian Composition Construction

In the first part of this section, up to Definition 2.4, only the ring $\mathbb{Z}$ will be under consideration; in this context, by a "binary quadratic form" will be meant a numerical binary Lagrangian quadratic form

$$[a, b, c] = [a, b, c]^L: \mathbb{Z}^2 \to \mathbb{Z}, \qquad {}^t(x, y) \mapsto ax^2 + bxy + cy^2$$

over $\mathbb{Z}$.

Lagrange's "Recherches d'arithmétique" [26, Vol. III, pp. 693–758] first introduced into number theory the notion of equivalence of binary quadratic forms, though not in the form of an explicit definition. Lagrange considered two forms

$$q = [a, b, c], \qquad q' = [a', b', c']$$

of the same nonzero discriminant as being not essentially different (since they represent the same set of integers, which was Lagrange's object of study) if there exists a 2×2 matrix T over $\mathbb{Z}$ such that

$$[a', b', c']\,({}^t(x, y)) = [a, b, c]\; T\,{}^t(x, y)) \tag{1}$$

for all x and y in $\mathbb{Z}$, and we shall find it convenient to say that in this case q and q' are *weakly equivalent*. It is easy to see that Lagrange's requirement that q and q' have the same discriminant is equivalent to the requirement that $\det T = \pm 1$. If we instead require that $\det T = +1$, we get the concept of *proper equivalence*, first introduced by Gauss in [22, Art. 158]. The distinction between these two types of equivalence is crucial for the theory of composition; it is the *proper* binary quadratic form-classes which are composed, and, as we shall see, it is

impossible to carry over the binary operation of composition to the grosser equivalence classes with respect to weak equivalence. This fact seems intimately connected with the major difficulties involved in constructing the operation of composition.

Dickson [15, Chap. III, Refs. 1–4] lists the following as the first historical steps towards Gauss' theory of composition.

Diophantus of Alexandria essentially asserts [16, III, Problem 22] (as usual, expressing himself only in terms of a special case: $65 = 5 \times 13$) that if two integers may each be written as a sum of two squares, their product may be written as a sum of two squares in two different ways; Dickson interprets this as indicating that Diophantus was in possession of the identity

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' \pm yy')^2 + (xy' \mp yx')^2. \tag{2a}$$

The generalization

$$(x^2 - ey^2)(x'^2 - ey'^2) = X^2 - eY^2, \tag{2b}$$

with

$$X = xx' + eyy', \quad Y = xy' + yx'$$

was used by the Hindu mathematician Brahmegupta (born 598 A.D.) and by Euler in their studies [7, 17] of Pell's equation. Euler generalized this further [20, Chap. II, Sects. 173–180] to

$$(ax^2 + cy^2)(x'^2 + acy'^2) = aX^2 + cY^2, \tag{2c}$$

with

$$X = xx' - cyy', \quad Y = axy' + yx'.$$

Dickson cites [15, Chap. 3, Ref. 3] two similar identities due to A. J. Lexell (1740–1784). Dickson also mentions in this list some work of Legendre, which we shall discuss in more detail in the historical note at the end of this section. Dickson's list omits the following composition identity, published by Lagrange in his additions [26, Vol. 7, Sect. IX, Art. 87, p. 166] to a translation of an algebra text by Euler which contains (2b):

$$(x^2 + axy + by^2)(x'^2 + ax'y' + by'^2) = X^2 + aXY + bY^2 \tag{2d}$$

with

$$X = xx' - byy', \quad Y = xy' + yx' + ayy'.$$

Presumably on the basis of this last identity, Bourbaki [6, p. 153] erroneously attributes to Lagrange most of the credit for originating Gauss' concept of composition; this point also will be discussed further at the end of this section.

Such identities as (2a), (2c), etc., suggest saying that in some sense [1, 0, 1] is a product of [1, 0, 1] and [1, 0, 1], [a, 0, c] is a product of [a, 0, c] and [1, 0, ac],

etc. Two difficulties arise in attempting to make this notion precise: uniqueness and existence of this "product." We next consider the question of uniqueness.

Given a "composition identity"

$$(ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2) = AX^2 + BXY + CY^2 \tag{3}$$

with

$$\begin{aligned} X &= m_0xx' + m_1xy' + m_2yx' + m_3yy', \\ Y &= n_0xx' + n_1xy' + n_2yx' + n_3yy', \end{aligned} \tag{4}$$

we shall say: $[A, B, C]$ *is transformed into the product of* $[a, b, c]$ *and* $[a', b', c']$ *by the substitution given by the matrix*

$$\Sigma = \begin{pmatrix} m_0, & m_1, & m_2, & m_3 \\ n_0, & n_1, & n_2, & n_3 \end{pmatrix}. \tag{5}$$

EXAMPLE 1. (2c) asserts that $[a, 0, c]$ is transformed into the product of $[a, 0, c]$ and $[1, 0, ac]$ by the substitution given by the matrix

$$\begin{pmatrix} 1, & 0, & 0, & -c \\ 0, & a, & 1, & 0 \end{pmatrix}.$$

Suppose that $[A, B, C]$ is transformed into the product of $[a, b, c]$ and $[a', b', c']$ by the substitution given by the matrix Σ. Suppose also that

$$[A, B, C] = [A', B', C'] \circ \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

i.e., that

$$AX^2 + BXY + CY^2 = A'X'^2 + B'X'Y' + C'Y'^2,$$

where

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha X + \beta Y \\ \gamma X + \delta Y \end{pmatrix}. \tag{6}$$

Then we also have the composition identity

$$(ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2) = A'X' + B'X'Y' + C'Y'^2,$$

where X' and Y' are given by (4) and (6). Thus, $[A', B', C']$ is transformed into the product of $[a, b, c]$ and $[a', b', c']$ by the substitution given (it is easily seen) by the matrix

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \Sigma. \tag{7}$$

The converse also holds; indeed, letting

$$\xi = {}^t(xx', xy', yx', yy')$$

we see that the three following statements are equivalent:

(a) $[A', B', C'] \circ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is transformed into the product of the forms q and q' by the substitution given by Σ.

(b) $q\begin{pmatrix} x \\ y \end{pmatrix} q'\begin{pmatrix} x' \\ y' \end{pmatrix} = [A'B'C']\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\Sigma\xi\right)$.

(c) $[A', B', C']$ is transformed into the product of q and q' by the substitution given by $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)\Sigma$.

In order to guarantee as much uniqueness as possible in the "product" we are trying to define, we must therefore restrict ourselves in (5) to 2×4 matrices which cannot be "factored" in the form (7) over $\mathbb{Z}$. The following lemma gives a restatement of this condition.

LEMMA 2.1. *Let Σ be a 2×4 matrix over $\mathbb{Z}$. We may write*

$$\Sigma = T\Sigma_1$$

with T a noninvertible 2×2 matrix over $\mathbb{Z}$ and Σ_1 a 2×4 matrix over $\mathbb{Z}$, unless the 2×2 subdeterminants of Σ have g.c.d. 1.

Proof. This is an easy consequence of the fact that there exist 2×2 and 4×4 invertible matrices P and Q, respectively, over $\mathbb{Z}$ such that

$$P\Sigma Q = \begin{pmatrix} d_1, & 0, & 0, & 0 \\ 0, & d_2, & 0, & 0 \end{pmatrix} = \begin{pmatrix} d_1, & 0 \\ 0, & d_2 \end{pmatrix}\begin{pmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \end{pmatrix},$$

where d_1 is the g.c.d. of the entries in Σ and d_1d_2 is the g.c.d. of the 2×2 subdeterminants of Σ. [Note also that if T is an *invertible* 2×2 matrix over $\mathbb{Z}$, then any 2×4 matrix Σ over $\mathbb{Z}$ has the trivial "factorization" $\Sigma = T(T^{-1}\Sigma)$.]

We are thus led to the following definition.

DEFINITION 2.1. A 2×4 matrix over $\mathbb{Z}$ will be called unimodular if its 2×2 subdeterminants have g.c.d. 1. The binary quadratic form $[A, B, C]^L$ will be called a *Legendre composite* of the forms $[a, b, c]^L$ and $[a', b', c']^L$ if it is transformed into their product by the substitution given by a unimodular 2×4 matrix over $\mathbb{Z}$.

Remark. The preceding argument also shows that the Σ_1 of Lemma 2.1 may be chosen to be unimodular.

EXAMPLE 2. Substituting $e = -4$ in (2b) gives the composition identity

$$(x^2 + 4y^2)(x'^2 + 4y'^2) = X^2 + 4Y^2,$$

with

$$X = xx' - 4yy', \quad Y = xy' + yx'$$

whence the composition identity

$$(x^2 + 4y^2)(x'^2 + 4y'^2) = X^2 + Y_1^2,$$

with

$$X = xx' - 4yy',\ Y_1(= 2Y) = 2xy' + 2yx'$$

(arising from the preceding identity because $[1, 0, 1]^L \circ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) = [1, 0, 4]^L$). Thus, both $[1, 0, 4]^L$ and $[1, 0, 1]^L$ are transformed into the product of $[1, 0, 4]^L$ with $[1, 0, 4]^L$ by the substitutions given respectively by the matrices

$$\Sigma_1 = \begin{pmatrix} 1, & 0, & 0, & -4 \\ 0, & 1, & 1, & 0 \end{pmatrix} \quad \text{and} \quad \Sigma = \begin{pmatrix} 1, & 0 \\ 0, & 2 \end{pmatrix} \Sigma_1 = \begin{pmatrix} 1, & 0, & 0, & -4 \\ 0, & 2, & 2, & 0 \end{pmatrix}$$

Σ_1 is unimodular but Σ is not, and correspondingly, $[1, 0, 4]^L$ is a Legendre composite of $[1, 0, 4]^L$ and $[1, 0, 4]^L$ but (it may be shown) $[1, 0, 1]^L$ is not.

EXAMPLE 3. In (2c), the matrix

$$\begin{pmatrix} 1, & 0, & 0, & -c \\ 0, & a, & 1, & 0 \end{pmatrix}$$

involved (cf. Example 1) is unimodular; thus, $[a, 0, c]^L$ is a Legendre composite of $[a, 0, c]$ and $[1, 0, ac]$.

It is easily seen from the discussion preceding Lemma 2.1 that if Q is a Legendre composite of q and q', so is any form weakly equivalent to Q. This mild degree of nonuniqueness does not seem too bad, especially since it is also easy to show that if Q is a Legendre composite of q and q', it is also a Legendre composite of any two forms weakly equivalent to q and q', respectively. It would seem that we need only pass to weak equivalence classes, obtaining a binary operation which combines the class of q and the class of q' to produce the class of any Legendre composite of q and q'. By a stroke of bad luck (i.e., because we are not yet going about things correctly) this falls just short of working: The set of all Legendre composites of two given forms is, when nonempty, not necessarily a *single* weak equivalence class; it may consist of *two* distinct weak equivalence classes (and, it may be proved, never more than two).

EXAMPLE 4. The forms [2, 1, 3] and [2, 1, 3] have both [2, 1, 3] and [1, 1, 6] as Legendre composites, and the latter two are not weakly equivalent. In more detail: a straightforward computation verifies that [2, 1, 3] and [1, 1, 6] are transformed into the product of [2, 1, 3] with itself by the substitutions given respectively by the unimodular matrices

$$\begin{pmatrix} 1, & -1, & -1, & -2 \\ -1, & -1, & -1, & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2, & 0, & 1, & 3 \\ 0, & 1, & -1, & 0 \end{pmatrix}.$$

Weakly equivalent forms represent the same integers; thus, [1, 1, 6], which represents 1, is not weakly equivalent to [2, 1, 3], since

$$2x^2 + xy + 3y^2 = 1, \qquad \text{i.e.,} \quad (4x + y)^2 + 23y^2 = 8$$

has no solution with x and y in $\mathbb{Z}$.

We have just encountered what is, in a way, the central difficulty in defining the notion of composition over the ring of integers. To overcome it, a modification of Definition 2.1 is needed which is much less straightforward, and involves a much deeper insight into the nature of composition identities. We first require the following marvelous theorem of Gauss, which gives a "universal composition identity" yielding (except for certain degenerate identities in which forms are perfect squares) all composition identities as special cases; roughly speaking, this theorem shows that (up to constant multiples) there is a unique composition identity associated with any given nonsingular 2×4 matrix Σ over $\mathbb{Z}$ (and not involving forms of discriminant 0).

THEOREM 2.2 (Gauss, [22, Art. 235]). *Let*

$$\Sigma = \begin{pmatrix} m_0, & m_1, & m_2, & m_3 \\ n_0, & n_1, & n_2, & n_3 \end{pmatrix}$$

be any 2×4 *matrix over* $\mathbb{Z}$; *then the binary quadratic form*

$$Q_\Sigma = [n_1n_2 - n_0n_3, m_0n_3 + m_3n_0 - m_1n_2 - m_2n_1, m_1m_2 - m_0m_3] \tag{8}$$

is transformed into the product of

$$q_\Sigma = [m_0n_1 - m_1n_0, m_0n_3 - m_3n_0 - m_1n_2 + m_2n_1, m_2n_3 - m_3n_2] \tag{9}$$

and

$$q'_\Sigma = [m_0n_2 - m_2n_0, m_0n_3 - m_3n_0 + m_1n_2 - m_2n_1, m_1n_3 - m_3n_1] \tag{10}$$

by the substitution given by Σ. *The three forms* Q_Σ, q_Σ, *and* q'_Σ *have the same discriminant.*

Conversely, if the binary quadratic form Q is transformed into the product of the binary quadratic forms q and q' by the substitution given by Σ, and if each of the forms q and q' has nonzero discriminant, then there exist rational numbers r and r' such that

$$q = rq_\Sigma, \quad q' = r'q'_\Sigma, \quad Q = rr'Q_\Sigma.$$

Proof. We begin by investigating in some detail the substitution (4) determined by Σ.

Let us solve (4) for x and y. Writing (4) in the form

$$\begin{aligned} X &= (m_0x' + m_1y')x + (m_2x' + m_3y')y, \\ Y &= (n_0x' + n_1y')x + (n_2x' + n_3y')y \end{aligned}$$

and noting that the determinant

$$\begin{vmatrix} m_0x' + m_1y', & m_2x' + m_3y' \\ n_0x' + n_1y', & n_2y' + n_3y' \end{vmatrix}$$

is exactly $q'_\Sigma\binom{x'}{y'} = q'_\Sigma$, we readily obtain

$$\begin{aligned} xq'_\Sigma &= n_2Xx' + n_3Xy' - m_2Yx' - m_3Yy', \\ yq'_\Sigma &= -n_0Xx' - n_1Xy' + m_0Yx' + m_1Yy'. \end{aligned} \tag{11}$$

Note the similarity between (4) and (11).

Similarly, we may solve (4) for x' and y' obtaining

$$\begin{aligned} x'q_\Sigma &= n_1Xx + n_3Xy - m_1Yx - m_3Yy, \\ y'q_\Sigma &= -n_0Xx - n_2Xy + m_0Yx + m_2Yy. \end{aligned} \tag{12}$$

We have passed from (4) to (11) and to (12). Naturally, if we pass directly from (11) to (12), i.e., solve (11) for x' and y', we should obtain the same result. As we shall now see, this simple insight into (4) immediately yields Gauss' composition identity

$$q_\Sigma\binom{x}{y}\, q'_\Sigma\binom{x'}{y'} = Q_\Sigma\binom{x}{y} \qquad \text{(where } X, Y \text{ are given by (4))}. \tag{13}$$

This elegant and illuminating derivation of (13) is due to Speiser [32, pp. 375–395].

Indeed, let us now solve (11) for x' and y' and compare the result with (12). Writing (11) in the form

$$\begin{aligned} xq'_\Sigma &= (n_2X - m_2Y)x' + (n_3X - m_3Y)y', \\ yq'_\Sigma &= (-n_0X + m_0Y)x' + (-n_1X + m_1Y)y' \end{aligned}$$

and noting that

$$\begin{vmatrix} n_2X - m_2Y, & n_3X - m_3Y \\ -n_0X + m_0Y, & -n_1X + m_1Y \end{vmatrix} = -Q_\Sigma \begin{pmatrix} x \\ y \end{pmatrix}$$

we obtain

$$\begin{aligned} x'Q_\Sigma &= q'_\Sigma(n_1Xx + n_3Xy - m_1Yx - m_3Yy), \\ y'Q_\Sigma &= q'_\Sigma(-n_0Xx - n_2Xy + m_0Yx + m_2Yy). \end{aligned} \tag{14}$$

Comparing with (12) we see that $x'Q_\Sigma = q'_\Sigma(x'q_\Sigma)$, i.e., (13) holds as asserted.

The following proof of the converse part of Gauss' theorem is due to Smith [31, pp. 232–234]. The idea is simply to take the discriminant of both sides of (3), considered as quadratic forms in x and y alone (and similarly for x' and y'). In more detail:

Suppose that $Q = [A, B, C]$ is transformed into the product of $q = [a, b, c]$ and $q' = [a', b', c']$ by the substitution given by Σ, i.e., suppose that (3) and (4) hold. Suppose also that q and q' have nonzero discriminants.

Let us temporarily treat x' and y' as constants in (3) and (4). We may then regard (4) as a linear substitution

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix},$$

where

$$\begin{aligned} \alpha &= m_0x' + m_1y', \quad \beta = m_2x' + m_3y', \\ \gamma &= n_0x' + n_1y', \quad \delta = n_2x' + n_3y'. \end{aligned}$$

Equation (3) then asserts the following equality between two binary quadratic forms in x and y (with coefficients in $\mathbb{Z}[x', y']$):

$$(ax^2 + bxy + cy^2)\, q' \begin{pmatrix} x' \\ y' \end{pmatrix} = [A, B, C] \left(\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right)$$

whence, taking the discriminant of both sides,

$$(b^2 - 4ac) \left[q' \begin{pmatrix} x' \\ y' \end{pmatrix} \right]^2 = (B^2 - 4AC) \begin{vmatrix} \alpha, & \beta \\ \gamma, & \delta \end{vmatrix}^2.$$

As we have already noted, $\alpha\delta - \beta\gamma = q'_\Sigma\binom{x'}{y'}$, so

$$(b^2 - 4ac) \left[q' \begin{pmatrix} x' \\ y' \end{pmatrix} \right]^2 = (B^2 - 4AC) \left[q'_\Sigma \begin{pmatrix} x' \\ y' \end{pmatrix} \right]^2. \tag{15}$$

By hypothesis, $b^2 - 4ac \neq 0$, so it follows from (14) that $q' = r'q'_\Sigma$ for some rational number r'. A similar argument shows that $q = rq_\Sigma$ for some rational number r. Then

$$Q\binom{X}{Y} = q\binom{x}{y}\, q'\binom{x'}{y'} = rr' q_\Sigma \binom{x}{y}\, q'_\Sigma \binom{x'}{y'} = rr' Q_\Sigma \binom{X}{Y} \tag{16}$$

by (3) and (13), where X and Y are given by (4). Now, as x, y, x', and y' range independently over the set Q of rational numbers, $\binom{X}{Y}$ as given by (4) ranges over all of Q^2; namely, given rational numbers X and Y we may solve (4) for rational x, y, x', and y' by first picking x' and y' so $q'_\Sigma\binom{x'}{y'} \neq 0$ (q'_Σ is not identically 0 since by hypothesis $q' = r'q'_\Sigma$ has nonzero discriminant) and then taking the values of x and y given by (11). Hence, (16) implies that $Q = rr'Q_\Sigma$.

Finally, we must prove that q_Σ, q'_Σ, and Q_Σ have the same discriminant. This may be verified from (8), (9), and (10) by a direct computation; it may also the proved as follows. Substituting

$$q = q_\Sigma, \quad q' = q'_\Sigma, \quad Q = Q_\Sigma$$

in (15) we see that q_Σ and Q_Σ have the same discriminant when $q'_\Sigma \neq 0$, hence, when the entries m_0, m_1,..., n_3 of Σ are indeterminates over $\mathbb{Z}$; hence, always. Similarly, q'_Σ and Q_Σ have the same discriminant.

Historical note. The first part of Theorem 2.2 (i.e., (13)) could, of course, be proved directly by a long and straightforward computation; indeed, Gauss leaves its verification to the reader. Speiser's proof was preferred in this presentation, on the grounds that deriving a formula this complicated and fundamental is preferable to simply verifying it. Gauss' demonstration of the converse part of Theorem 2.2 in [22, Art. 235] is extremely difficult; the simplification involved in the proof of Smith presented here was considerable. The first simplification of Gauss' argument was achived by Bazin [4]; Bazin's proof, which appeared 50 years after the publication of Gauss', involves an earlier form of the idea in Smith's proof, consisting of setting $x' = 1$, $y' = 0$ in (3) and then taking the discriminant of both sides. The same idea as Bazin's occurs in a rather later paper of Arndt. [1]. The source of these reference was [15, Chap. III, Refs. 13, 16, 19, and 46].

DEFINITION 2.2. The binary quadratic form Q will be called a *Gaussian composite* of the binary quadratic forms q and q' if there exists a unimodular 2×4 matrix Σ over $\mathbb{Z}$ such that

$$Q = Q_\Sigma, \quad q = q_\Sigma, \quad q' = q'_\Sigma$$

(where Q_Σ, q_Σ, q'_Σ are defined by Eqs. (5), (8), (9), and (10)).

EXAMPLE 5. Letting Σ denote the unimodular matrix

$$\Sigma = \begin{pmatrix} 1, & 0, & 0, & -c \\ 0, & a, & 1, & 0 \end{pmatrix}$$

we see (cf. Example 3) that $Q_\Sigma = [a, 0, c]$ is a Gaussian composite of $q_\Sigma = [a, 0, c]$ and $q'_\Sigma = [1, 0, ac]$. More generally, if

$$S = \begin{pmatrix} 1, & 0, & 0, & -c \\ 0, & a, & a', & b \end{pmatrix}$$

then

$$Q_S = [aa', b, c],\ q_S = [a, b, a'c],\ q'_S = [a', b, ac].$$

If a, a' and b have g.c.d. 1, then S is unimodular and $[aa', b, c]$ is a Gaussian composite of $[a, b, a'c]$ and $[a', b', ac]$.

EXAMPLE 6 (cf. Example 4). The unimodular matrices

$$\begin{pmatrix} 1, & -1, & -1, & -2 \\ 1, & 1, & 1, & -1 \end{pmatrix},\ \begin{pmatrix} 2, & 0, & 1, & 3 \\ 0, & 1, & -1, & 0 \end{pmatrix},\ \text{and}\ \begin{pmatrix} 2, & 0, & -1, & -3 \\ 0, & 1, & 1, & 0 \end{pmatrix}$$

exhibit.

$[2, -1, 3]$ as a Gaussian composite of $[2, 1, 3]$ and $[2, 1, 3]$,

$[-1, -1, -6]$ as a Gaussian composite of $[2, 1, 3]$ and $[-2, -1, -3]$,

$[1, 1, 6]$ as a Gaussian composite of $[2, -1, 3]$ and $[2, 1, 3]$.

It is clear from Theorem 2.2 that a Gaussian composite is also a Legendre composite; however, the converse is not true. The much deeper Definition 2.2 is free of the defects of the more simple-minded Definition 2.1 If two binary quadratic forms q and q' possess a Gaussian composite, it may be proved that the set of all their Gaussian composites is a *single* proper numerical form-class. Since also any forms q_1, q'_1 properly equivalent to q, q', respectively, have the same set of Gaussian composites as do q and q', Gaussian composition passes over to a (not always defined) binary operation on proper numerical form-classes. Gauss proved these assertions in [22, Arts. 236–239] together with the following fact: The binary quadratic forms $[a, b, c]$ and $[a', b', c']$ possess a Gaussian composite if and only if they are comaximal (i.e., the numbers a, b, c, a', b', c' have g.c.d. 1) and have the same discriminant.

DEFINITION 2.3. Let α and β be two proper numerical L form-classes over $\mathbb{Z}$ which are comaximal and have the same discriminant; by their *composite* $\alpha\beta$ will

be meant the proper numerical L form-class consisting of all Gaussian composites of a form in α with a form in β.

Finally, in ([22, Arts. 174, 175, 185, 240, 243] Gauss established what amounts to the following theorem:

THEOREM 2.3. *Let $G(\delta)$ denote the set of all primitive proper numerical L form-classes over $\mathbb{Z}$ of discriminant δ; then $G(\delta)$ forms a finite Abelian group under composition.*

This is the beautiful and masterly construction of Gauss, the generalization of which is the purpose of the present paper. We note next the following important generalization, first suggested by Butts and Estes in [9], and studied in detail by Dulin and Butts in [8].

DEFINITION 2.4. Let R be any ring, and let

$$\Sigma = \begin{pmatrix} m_0 , & m_1 , & m_2 , & m_3 \\ n_0 , & n_1 , & n_2 , & n_3 \end{pmatrix}$$

be a 2×4 matrix over R; then we denote by Q_Σ , q_Σ , and q'_Σ respectively the following numerical binary Lagrangian quadratic forms over R:

$$Q_\Sigma = [n_1n_2 - n_0n_3 , m_0n_3 + m_3n_0 - m_1n_2 - m_2n_1 , m_1m_2 - m_0m_3],$$

$$q_\Sigma = [m_0n_1 - m_1n_0 , m_0n_3 - m_3n_0 - m_1n_2 + m_2n_1 , m_2n_3 - m_3n_2],$$

$$q'_\Sigma = [m_0n_2 - m_2n_0 , m_0n_3 - m_3n_0 + m_1n_2 - m_2n_1 , m_1n_3 - m_3n_1].$$

We say that Σ is *unimodular* over R if its six 2×2 subdeterminants generate the unit ideal in R. Given three numerical binary Lagrangian quadratic forms Q, q, and q' over R, we say that Q is a Gaussian composite of q and q' over R when there exists a unimodular 2×4 matrix Σ over R such that

$$Q = Q_\Sigma , \quad q = q_\Sigma , \quad q' = q'_\Sigma .$$

Remark. If R is a ring on which 2 is not a zero-divisor, this passes over to a (not always defined) binary operation on proper numerical form-classes over R, just as in the case $R = \mathbb{Z}$ [8, Proposition 2.16], but this fact will not be needed in the present paper. We shall, however, in Section 4, have occasion to use the three following results.

PROPOSITION 2.4. *Let*

$$\Sigma = \begin{pmatrix} m_0 , & m_1 , & m_2 , & m_3 \\ n_0 , & n_1 , & n_2 , & n_3 \end{pmatrix}$$

be a 2×4 *matrix over the ring* R; *then* Q_Σ, q_Σ, *and* q'_Σ *have the same discriminant and the same parity, and*

$$Q_\Sigma \begin{pmatrix} X \\ Y \end{pmatrix} = q_\Sigma \begin{pmatrix} x \\ y \end{pmatrix} q'_\Sigma \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{17}$$

holds, considered as an equation between elements of $R[x, y, x', y']$, *where*

$$X = m_0xx' + m_1xy' + m_2yx' + m_3yy',$$
$$Y = n_0xx' + n_1xy' + n_2yx' + n_3yy'.$$

Proof. The parities of Q_Σ, q_Σ, and q'_Σ are, by Definition 2.4, the residue classes respectively of

$$m_0n_3 + m_3n_0 - m_1n_2 - m_2n_1,$$
$$m_0n_3 - m_3n_0 - m_1n_2 + m_2n_1,$$

and

$$m_0n_3 - m_3n_0 + m_1n_2 - m_2n_1$$

in $R/2R$, and it is obvious these coincide. As for the remainder of Proposition 2.4, the relevant portions of the proof of Theorem 2.2 are still valid.

Remark. There are apparently two senses in which a "composition identity" (17) over a ring R may be interpreted: as asserting that the left-hand side and the right-hand side of (17) coincide considered as elements of $R[x, y, x', y']$, or as asserting that (17) holds for all x, y, x', and y' in R. Actually, these two senses coincide: It is obvious that if (17) holds in the first sense, then it holds in the second sense; to prove the converse implication, it suffies to prove that, if r_i $(1 \leqslant i \leqslant 9)$ are elements of R such that

$$r_1x^2x'^2 + r_2x^2x'y' + r_3x^2y'^2 + r_4xyx'^2 + r_5xyx'y' + r_6xyy'^2 + r_7y^2x'^2 + r_8y^2x'y' + r_9y^2y'^2 = 0 \tag{*}$$

for all x, y, x', y' in R, then all $r_i = 0$. This last statement follows immediately upon substituting the 16 special values

$$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) \qquad (\epsilon_i = 0 \text{ or } 1)$$

for (x, y, x', y') in (*).

PROPOSITION 2.5. *If two numerical binary Lagrangian quadratic forms* q *and* q' *over the ring* R *possess a Gaussian composite over* R, *then they are comaximal, i.e.,*

$$\mathrm{div}_R q + \mathrm{div}_R q' = R.$$

Remark. We recall from Section 1 that if $q = [a, b, c]$, $\mathrm{div}_R q = Ra + Rb + Rc$ is the ideal generated over R by $\{q(u)\colon u \in R^2\}$ (cf. Eq. (37) of Section 1 and the proof of Proposition 1.16).

Proof of Proposition 2.5. By hypothesis, there exists a 2×4 matrix

$$\Sigma = \begin{pmatrix} m_0 , & m_1 , & m_2 , & m_3 \\ n_0 , & n_1 , & n_2 , & n_3 \end{pmatrix}$$

over R satisfying the following three conditions:

(I) Σ is unimodular, i.e., the six elements

$$d_{ij} = m_i n_j - m_j n_i \qquad (0 \leqslant 1 < j \leqslant 3)$$

generate the unit ideal in R.

(II) $q = q_\Sigma = [d_{01} , d_{03} - d_{12} , d_{23}]$.

(III) $q' = q'_\Sigma = [d_{02} , d_{03} + d_{12} , d_{13}]$.

We must show that this implies the ideal

$$J = \mathrm{div}_R q + \mathrm{div}_R q'$$

equals R. J is generated over R by the six elements

$$d_{01} , d_{02} , d_{13} , d_{23} , d_{03} - d_{12} , d_{03} + d_{12} .$$

The Plücker identity

$$d_{01}d_{23} - d_{02}d_{13} + d_{03}d_{12} = 0$$

shows that J contains $d_{03}d_{12}$, and hence contains

$$d_{03}^2 = d_{03}d_{12} + (d_{03} - d_{12})d_{03} \qquad \text{and} \qquad d_{12}^2 = d_{03}d_{12} - (d_{03} - d_{12})d_{12} .$$

(I) shows there exist r and s in R with

$$I \equiv r d_{03} + s d_{12} \qquad (\mathrm{mod}\ J)$$

whence

$$I \equiv (r d_{03} + s d_{12})^2 \equiv 0 \qquad (\mathrm{mod}\ J),\ J = R.$$

THEOREM 2.6. *Let Q, q and q' be numerical binary L-quadratic forms over the ring R. If Q is a Gaussian composite of q and q' over R, then*

$$\mathrm{div}_R Q = (\mathrm{div}_R q)(\mathrm{div}_R q').$$

Proof. Let

$$\Sigma = \begin{pmatrix} m_0 , & m_1 , & m_2 , & m_3 \\ n_0 , & n_1 , & n_2 , & n_3 \end{pmatrix}$$

be a unimodular 2×4 matrix over R; we are done if we can show that

$$\operatorname{div}_R Q_\Sigma = (\operatorname{div}_R q_\Sigma)(\operatorname{div}_R q'_\Sigma).$$

Let

$$Q_\Sigma = [A, B, C],\ q_\Sigma = [a, b, c],\ q'_\Sigma = [a', b', c'];$$

then

$$\operatorname{div}_R Q_\Sigma = RA + RB + RC$$

while $(\operatorname{div}_R q_\Sigma)(\operatorname{div}_R q'_\Sigma)$ is generated over R by the nine products

$$aa',\ ab',\ ac',\ ba',\ bb',\ bc',\ ca',\ cb',\ cc'. \tag{18}$$

The inclusion

$$\operatorname{dig}_R Q_\Sigma \supseteq (\operatorname{div}_R q_\Sigma)(\operatorname{div}_R q'_\Sigma)$$

follows from the fact that $(\operatorname{div}_R q_\Sigma)(\operatorname{div}_R q'_\Sigma)$ is generated over R by the set of all products

$$q_\Sigma \begin{pmatrix} x \\ y \end{pmatrix} q'_\Sigma \begin{pmatrix} x' \\ y' \end{pmatrix}$$

with x, y, x', and y' in R; by Gauss' composition identity (Proposition 2.4) every such product is in the range of Q_Σ, and thus in $\operatorname{div}_R Q_\Sigma$.

Thus, each of the nine products in (18) is a linear combination over R of A, B, and C; for later use in this proof, it is convenient to now exhibit this fact explicitly by means of the following nine equations, obtained by equating corresponding powers of x, y, x', and y' on both sides of Gauss' composition identity (17):

$$aa' = Am_0^2 + Bm_0n_0 + Cn_0^2, \tag{19}$$

$$ac' = Am_1^2 + Bm_1n_1 + Cn_1^2, \tag{20}$$

$$ca' = Am_2^2 + Bm_2n_2 + Cn_2^2, \tag{21}$$

$$cc' = Am_3^2 + Bm_3n_3 + Cn_3^2, \tag{22}$$

$$ab' = 2Am_0m_1 + B(m_0n_1 + m_1n_0) + 2Cn_0n_1, \tag{23}$$

$$ba' = 2Am_0m_2 + B(m_0n_2 + m_2n_0) + 2Cn_0n_2, \tag{24}$$

$$bc' = 2Am_1m_3 + B(m_1n_3 + m_3n_1) + 2Cn_1n_3, \tag{25}$$

$$cb' = 2Am_2m_3 + B(m_2n_3 + m_3n_2) + 2Cn_2n_3, \tag{26}$$

$$bb' = 2A(m_0m_3 + m_1m_2) + B(m_0n_3 + m_3n_0 + m_1n_2 + m_2n_1) + 2C(n_0n_3 + n_1n_2) \tag{27}$$

(cf. Eqs. [1]–[9] in [22, Art. 235]). Let us, in particular, consider Eq. (27), which results from equating the coefficients of $xyx'y'$ on both sides of (17). Gauss proceeded to break up the right-hand side of (27) into the following expressions:

$$\Lambda_1 = 2Am_0m_3 + B(m_0n_3 + m_3n_0) + 2Cn_0n_3\,, \tag{28}$$

$$\Lambda_2 = 2Am_1m_2 + B(m_1n_2 + m_2n_1) + 2Cn_1n_2 \tag{29}$$

(presumably, his motivation for so doing was the following one: As compared with the preceding eight equations, (27) has unusually many terms because $xyx'y'$ may be written in the two forms $(xx')(yy')$ and $(xy')(yx')$, and accordingly the contributions to the coefficient of $xyx'y'$ in the left-hand side of (17) break up into Λ_1 and Λ_2). Thus, (27) becomes

$$bb' = \Lambda_1 + \Lambda_2\,. \tag{27a}$$

Though we do not require them for the present proof, we note the following identities due to Gauss (cf. [22, Art. 235], Eqs. [10], [11] and the discussion following them):

$$2\Lambda_1 = bb' + \delta, \tag{30}$$

$$2\Lambda_2 = bb' - \delta, \tag{31}$$

where δ is the common discriminant of q_Σ, q'_Σ, and Q_Σ; these may be verified by direct substitution from Definition 2.4.

We shall make use of the preceding formulas in proving the inclusion

$$\operatorname{div}_R Q_\Sigma \subseteq (\operatorname{div} q_\Sigma)(\operatorname{div} q'_\Sigma),$$

i.e., in proving that A, B, and C are linear combinations over R of the nine products in (18). We begin by showing that A is such a linear combination.

Let d_{ij} denote the subdeterminant $m_in_j - m_jn_i$ of Σ. From Eqs. (19) through (29), Gauss derived the following six equations [22, Art. 235, the discussion preceding Conclusion Five]:

$$\mathrm{Ad}_{01}^2 = a(a'n_1^2 - b'n_0n_1 + c'n_0^2), \tag{32}$$

$$\mathrm{Ad}_{02}^2 = a'(an_2^2 - bn_0n_2 + cn_0^2), \tag{33}$$

$$\mathrm{Ad}_{03}^2 = aa'n_3^2 - \Lambda_1n_0n_3 + cc'n_0^2, \tag{34}$$

$$\mathrm{Ad}_{12}^2 = ac'n_2^2 - \Lambda_2n_1n_2 + ca'n_1^2, \tag{35}$$

$$\mathrm{Ad}_{13}^2 = c'(an_3^2 - bn_1n_3 + cn_1^2), \tag{36}$$

$$\mathrm{Ad}_{23}^2 = c(a'n_3^2 - b'n_2n_3 + c'n_2^2) \tag{37}$$

[for example, we obtain Eq. (32) for $\mathrm{Ad}_{01}^2 = A(m_0n_1 - m_1n_0)^2$ upon multiplying (19) by n_1^2, (23) by $-n_0n_1$, (20) by n_0^2, and then adding; the remainder are obtained similarly].

Gauss then proceeded to reason approximately as follows in the case $R = \mathbb{Z}$ [22, Art. 235]; his proof remains valid for R any PID of characteristic $\neq 2$, and requires the additional assumption that neither q_Σ nor q'_Σ is the form $[0, 0, 0]^L$. To show that the ideal $(\mathrm{div}_R q_\Sigma)(\mathrm{div}_R q'_\Sigma)$ contains A, it suffices to show this ideal contains the quantities in (32) through (37) (since the d_{ij}^2 generate the unit ideal); it thus suffices to show that this ideal contains Λ_1 and Λ_2, since it contains all the products in (18). Now, R being a PID, let

$$(\mathrm{dig}_R\, q_\Sigma)(\mathrm{div}_R\, q_\Sigma) = dR$$

with d in R; then d divides every product in (18), and our assumption that neither q_Σ nor q'_Σ is $[0, 0, 0]$ implies

$$\mathrm{div}_R\, q_\Sigma \neq 0,\ \mathrm{div}_R\, q'_\Sigma \neq 0, \qquad d \neq 0.$$

Λ_1/d and Λ_2/d are elements of the quotient field of R whose sum (cf. (27a))

$$\Lambda_1/d + \Lambda_2/d = bb'/d$$

and product (we here use (30) and (31))

$$\begin{aligned}\Lambda_1\Lambda_2/d^2 &= (b^2b'^2 - \delta^2)/4d^2 = b^2(b'^2 - \delta)/4d^2 + \delta(b^2 - \delta)/4d^2\\ &= b^2a'c'/d^2 + (b'^2 - 4a'c')\,ac/d^2\end{aligned}$$

both lie in R. Since R is integrally closed, Λ_1/d and Λ_2/d lie in R, i.e., Λ_1 and Λ_2 lie in $(\mathrm{div}_R q_\Sigma)(\mathrm{div}_R q'_\Sigma)$.

The preceding proof, that Λ_1 and Λ_2 (and hence A) lie in the ideal $(\mathrm{div}_R q_\Sigma)$ $(\mathrm{div}_R q'_\Sigma)$, breaks down if R is not a PID. We may, in the general case, make use instead of the weaker fact that $\Lambda_1 d_{03}$ and $\Lambda_2 d_{12}$ lie in this ideal. Namely, we have the identities

$$\Lambda_1 d_{12} = a'bc' - ab'c, \tag{38}$$

$$\Lambda_2 d_{03} = a'bc' + ab'c, \tag{39}$$

$$\Lambda_1 d_{03} = bb'd_{03} - a'bc' - ab'c, \tag{40}$$

$$\Lambda_2 d_{12} = bb'd_{12} - a'bc' + ab'c. \tag{41}$$

Since, by (27a), $\Lambda_1 + \Lambda_2 = bb'$, to prove these four identities it suffices to verify (38) and (39), which we may do by direct substitution from (28), (29), and Definition 2.4; e.g., both sides of (38) then become

$$\begin{aligned}&m_0^2m_1n_2n_3^2 - m_2m_3^2n_0^2n_1 - m_0^2m_2n_1n_3^2 + m_1m_3^2n_0^2n_2 - m_0m_1^2n_2^2n_3\\ &\quad + m_2^2m_3n_0n_1^2 - 2m_0m_1m_3n_0n_2n_3 + 2m_0m_2m_3n_0n_1n_3\\ &\quad + 2m_0m_1m_3n_1n_2^2 - 2m_1m_2^2n_0n_1n_3 + m_0m_2^2n_1^2n_3 - m_1^2m_3n_0n_2^2\\ &\quad - 2m_0m_2m_3n_1^2n_2 + 2m_1^2m_2n_0n_2n_3\,.\end{aligned}$$

[Or again, if we are willing to first verify (30) and (31), we may instead reason as follows: since (38) and (39) amount to polynomial identities with integral coefficients in the entries m_0, m_1,..., n_3 of Σ, it suffices to prove them in the case $R = \mathbb{Z}$, when they follow by dividing by 4 both sides of

$$4\Lambda_1 d_{12} = (bb' + \delta)(b' - b) = b(b'^2 - \delta) - b'(b^2 - \delta) = 4a'bc' - 4ab'c$$

and of

$$4\Lambda_2 d_{03} = (bb' - \delta)(b' + b) = b(b'^2 - \delta) + b'(b^2 - \delta) = 4a'bc' + 4ab'c.]$$

Let J be the ideal generated over R by

$$d_{03}^3, d_{12}^3, d_{01}^2, d_{02}^2, d_{13}^2, d_{23}^2;$$

then Eqs. (32) through (37), together with (40) and (41), show that

$$AJ \subseteq (\mathrm{div}_R\, q_\Sigma)(\mathrm{dig}_R\, q'_\Sigma).$$

Since by hypothesis Σ is unimodular, there exist r_{ij} in R with

$$\sum_{0 \leqslant i < j \leqslant 3} r_{ij} d_{ij} = 1.$$

Then

$$1 = \left(\sum_{i<j} r_{ij} d_{ij}\right)^9 \in J,$$

i.e., $J = R$, whence A belongs to $(\mathrm{div}_R q_\Sigma)(\mathrm{div}_R q'_\Sigma)$.

The following six equations (due to Gauss, [22, Art. 235]):

$$Bd_{01}^2 = -2aa'm_1n_1 + ab'(m_0n_1 + m_1n_0) - 2ac'm_0n_0, \tag{42}$$

$$Bd_{02}^2 = -2aa'm_2n_2 + ba'(m_0n_2 + m_2n_0) - 2ca'm_0n_0, \tag{43}$$

$$Bd_{03}^2 = -2aa'm_3n_3 + \Lambda_1(m_0n_3 + m_3n_0) - 2cc'm_0n_0, \tag{44}$$

$$Bd_{12}^2 = -2ac'm_2n_2 + \Lambda_2(m_1n_2 + m_2n_1) - 2ca'm_1n_1, \tag{45}$$

$$Bd_{13}^2 = -2ac'm_3n_3 + bc'(m_1n_3 + m_3n_1) - 2cc'm_1n_1, \tag{46}$$

$$Bd_{23}^2 = -2ca'm_3n_3 + cb'(m_2n_3 + m_3n_2) - 2cc'm_2n_2 \tag{47}$$

together with (40) and (41) show similarly that B is in $(\mathrm{div}_R q)(\mathrm{div}_R q')$. Finally, that C is in $(\mathrm{div}_R q)(\mathrm{div}_R q')$ follows in the same way from (40), (41), and the six equations involving Cd_{ij}^2 obtained from Eqs. (32) through (37) upon applying them to the matrix

$$\Sigma_0 = \begin{pmatrix} -n_3, & n_2, & n_1, & -n_0 \\ m_3, & -m_2, & -m_1, & m_0 \end{pmatrix}$$

in place of Σ. [Note that $q_{\Sigma_0} = [c, -b, a]$, $q'_{\Sigma_0} = [c', -b', a']$, $Q_{\Sigma_0} = [C, -B, A]$, $\Lambda_1(\Sigma_0) = \Lambda_1(\Sigma)$, $\Lambda_2(\Sigma_0) = \Lambda_2(\Sigma)$] Thus, $(\mathrm{div}_R q_\Sigma)(\mathrm{div}_R q'_\Sigma)$ contains $RA + RB + RC = \mathrm{div}_R Q_\Sigma$; since we have already proved the converse inclusion, this completes the proof of the theorem.

Remark. Professor André Weil has obtained a much more elegant proof of Theorem 2.6, based on Dedekind's "narrow ideal class" approach to composition. His proof shows a bit more: Even if Σ is not unimodular, we still have

$$\mathrm{div}_R Q_\Sigma = (\mathrm{div}_R q_\Sigma)(\mathrm{dig}_R q'_\Sigma) I^2,$$

where I is the ideal generated by the 2×2 minors of Σ. Still another proof of Theorem 2.6 (assuming $I = R$) is indicated in the remark following Lemma 4.14 below.

We conclude this section with the following historical note, in which it is to be understood that all forms considered are over $\mathbb{Z}$.

Historical note. To the author's best knowledge, all that was known of the theory of composition of binary quadratic forms, prior to the work of Gauss in [22], consisted of the few isolated composition identities cited at the beginning of this section, together with some work of A.M. Legendre which will next be discussed.

Dickson [15, Chap. III, Ref. 4], immediately after listing (2a) through (2c) together with their sources, cites Legendre as having proved in [27] the following result:

(2e) *If* $q = [a, b, c]$ and $q' = [a', b', c']$ *are forms of the same discriminant* δ, *and if* a *and* a' *are relatively prime, then there exists some composition identity transforming some form of discriminant* δ *into the product of* g *and* g'.

Dickson only cites Legendre's statement and proof of (2e) in the case that b and b' are both even, but in fact Legendre [27] also gives a separate proof for the remaining case.

However, in the present author's opinion, the contribution of Legendre in [27, Quatrième partie, Sect. III] was on a much deeper level than simply that of establishing (2e), i.e., establishing the existence of certain compsition identities with preassigned q and q'; namely, the first edition of [27] was the earliest published work in which the possibility was recognized of utilizing the phenomenon of composition identities for the purpose of constructing a binary operation on form-classes.

This fact is a bit obscured by Legendre's terminology in [27], where the phrase "diviseur quadratique de la formule $t^2 + au^2$" sometimes is to be interpreted as meaning a binary quadratic form of discriminant $-4a$ equal to that of $t^2 + au^2$, and sometimes is to be interpreted as meaning a weak form-class of that discriminant; also, Legendre's concept of composition of weak form-classes in [27] is nowhere stated explicitly in the form of a definition,

though what is meant becomes clear through a large number of numerical examples there given.

For instance, in subsection 373 [27] Legendre lists $A = y^2 + 2yz + 42z^2$, $B = 2y^2 + 2yz + 21z^2$, $C = 5y^2 + 6yz + 10z^2$, $D = 3y^2 + 2yz + 14z^2$, $E = 6y^2 + 2yz + 7z^2$, as the five "diviseurs quadratiques" of the form $t^2 + 41u^2$, by which he apparently means (though he nowhere mentions the notion of weak form-class) that these represent the five weak form-classes of discriminant equal to that of $t^2 + 41u^2$; he then gives a table containing all possible Legendre compositions of these weak form-classes, with such entries as

$$CC = \begin{cases} A \\ B \end{cases}, \quad DE = \begin{cases} B \\ C \end{cases}, \text{ etc.}$$

The following expresses more formally the notion of composition which, apparently, Legendre had in mind: Let α and β be weak form-classes which are of the same discriminant δ and which contain forms

$$q = [a, b, c] \qquad \text{and} \qquad q' = [a', b', c'],$$

respectively, such that a and a' are relatively prime. (The latter condition, it may be shown, is equivalent to the condition that α and β be comaximal.) By (2e), there exist forms Q of discriminant δ which are transformable into the product of q and q'; Legendre correctly asserts that there exist at most two such "diviseurs quadratiques," i.e., that the set of all such Q consists of at most two weak form-classes (though he only proves this fact in the special case for which a and a' are both prime numbers); the two-valued symbol $\alpha\beta$ is then used to denote either of the two weak form-classes containing such forms Q.

Suppose that q and q' are comaximal forms of the same discriminant δ, and that the form Q is transformed into the product of q and q' by the substitution associated with the matrix Σ. Using Theorem 2.2 and Proposition 2.5, it is easy to show that Q has discriminant δ if and only if Σ is unimodular. It follows immediately that (although neither Σ nor its unimodularity is mentioned in Legendre's discussion), the two-valued composition of Legendre is indeed that arising from the "Legendre composite" of Definition 2.1 upon passing to weak form-classes (and restricting to pairs which are comaximal and have the same discriminant).

Let us next compare the composition theory of Legendre (first published [27] in 1798) with that of Gauss (first published [22] in 1801). In contrast to Legendre's extremely sketchy treatment, Gauss' theory is developed in [22] with perfect mathematical rigor and overwhelming mathematical power, the group properties (an astonishingly modern touch) are established, the celebrated Duplication Theorem is proved, and applications of the theory are developed. Moreover, in itself, the Gaussian composition of proper form-classes lies on a much deeper level than Legendre's two-valued composition of weak form-classes; there is no

nontrivial way of improving the latter to obtain the former, a fact which constitutes an important and characteristic peculiarity of the whole subject. (The forgoing is to be understood as written, not in depreciation of Legendre's ingenious work, but rather in awe of Gauss'.) It seems difficult to tell whether Gauss was acquainted, when developing his own theory of composition, with the work of Legendre; in the preface to [22], Gauss wrote; "Since this book," i.e., Legendre's [27], "came to my attention after the greater part of my work was in the hands of the publishers, *I* was unable to refer to it in analogous parts of my book. *I* felt obliged, however, to add some observations in an Appendix and *I* trust that this understanding and illustrious man will not be offended"; the added observations mentioned deal only with topics other than composition, however. Gauss also asserts, at the beginning of [22, Art. 234]: "..., we will go on to another very important subject, the *composition* of forms. Thus far no one has considered this point."

So much for the historical relationship between Legendre's concept of composition and that of Gauss; the mathematical relationship is as follows. Let us say that two proper form-classes α and β are *weakly equivalent* if one (hence every) form in α is weakly equivalent to one (hence every) form in β. If we define the *opposite* of a proper form-class α to be the proper form-class

$$\alpha^{\mathrm{op}} = \{[a, -b, c] : [a, b, c] \in \alpha\}$$

and note that

$$[a, -b, c] = [a, b, c] \circ \begin{pmatrix} 1, & 0 \\ 0, & -1 \end{pmatrix}, \qquad \det \begin{pmatrix} 1, & 0 \\ 0, & -1 \end{pmatrix} = -1,$$

it is readily seen that the only proper form-classes weakly equivalent to α are α and α^{op}, and that the weak form-class containing α is $\alpha \cup \alpha^{\mathrm{op}}$. Also, noting that if the unimodular matrix

$$\Sigma = \begin{pmatrix} m_0\,, & m_1\,, & m_2\,, & m_3 \\ n_0\,, & n_1\,, & n_2\,, & n_3 \end{pmatrix}$$

exhibits $[A, B, C]$ as a Gaussian composite of $[a, b, c]$ and $[a', b', c']$, then the unimodular matrix

$$\begin{pmatrix} m_0\,, & -m_1\,, & -m_2\,, & m_3 \\ -n_0\,, & n_1\,, & n_2\,, & -n_3 \end{pmatrix}$$

exhibits $[A, -B, C]$ as the Gaussian composite of $[a, -b, c]$ and $[a', -b', c']$, it follows that

$$(\alpha\beta)^{\mathrm{op}} = (\alpha^{\mathrm{op}})(\beta^{\mathrm{op}}).$$

Hence, given two weak form-classes $\alpha \cup \alpha^{\mathrm{op}}$ and $\beta \cup \beta^{\mathrm{op}}$ which are comaximal and of the same discriminant, α and β denoting proper form-classes, the four composite proper-form-classes

$$\alpha\beta,\ \alpha^{\mathrm{op}}\beta,\ \alpha\beta^{\mathrm{op}} = (\alpha^{\mathrm{op}}\beta)^{\mathrm{op}},\ \alpha^{\mathrm{op}}\beta^{\mathrm{op}}$$

make up (at most) two weak form-classes

$$\alpha\beta \cup (\alpha\beta)^{\mathrm{op}}, \qquad \alpha^{\mathrm{op}}\beta \cup \alpha\beta^{\mathrm{op}}$$

which are readily proved to be the two Legendre composites of $\alpha \cup \alpha^{\mathrm{op}}$ and $\beta \cup \beta^{\mathrm{op}}$. Thus, the composition of Gauss is not compatible with weak equivalence, and gives rise to a "two-valued binary binary operation" upon passing to weak form-classes, which is the composition of Legendre.

In [6], Bourbaki makes the interesting point that (except for the usual binary operations on numbers) the composition of proper form-classes and the multiplication of permutations were the earliest sources of the basic abstract algebraic concept of a "loi de composition." However, the following inaccuracy occurs in Bourbaki's discussion of this topic, which (considering the respect in which Bourbaki's texts are justly held) would seem worth correcting. Bourbaki asserts [6, p. 153]: "Lagrange avait défini, dans l'ensemble des formes de même discriminant, une relation d'équivalence (*), et avait, d'autre part démontré une identité qui fournissait, dans cet ensemble, une loi de composition commutative (non partout définie); partant de ces résultats, Gauss montre que cette loi est compatible (au sens de Section 4) avec la relation d'équivalence précédente (V, t. 1, p. 272): « *On voit par là* », dit-il alors, « *ce qu'on doit entendre par une classe composée de deux ou de plusieurs classes* »" The notation (*) here refers to a footnote in which the "relation d'équivalence" is identified as proper equivalence.

If Bourbaki's assertion were correct, Gauss' contribution to the definition of composition would consist merley of a simple insight which completed a construction already more than half performed by Lagrange. This contradicts the assertion of Gauss [22, Art. 234] in which he specifically says if his theory of composition of forms, "Thus far no one has considered this point." In fact, the assertion of Bourbaki just quoted is in error in the following four respects:

(a) The only concept of equivalence of binary quadratic forms available to Lagrange was that of weak equivalence; proper equivalence first appeared in the literature in Gauss [22]. In discussing the work of Lagrange and Legendre on quadratic forms, Gauss asserted [22, Art. 222]: "Thus far no one," i.e., no one before Gauss, "has used the distinction between proper and improper equivalence, but it is a very effective instrument for more subtle investigations."

(b) To the present author's best knowledge, there exists in the literature no binary operation ("loi de composition") of the sort mentioned by Bourbaki

on the set of forms over $\mathbb{Z}$ of a given discriminant. Rather, there is the ternary relation given by Definition 2.2

$$Q \text{ is a Gaussian composite of } q \text{ and } q'$$

which only upon passage to proper form-classes yields the binary operation

$$(\text{cls } q)(\text{cls } q') = \text{cls } Q.$$

(c) The composition identity used by Gauss to compose proper form-classes is not Lagrange's identity (2d), but rather the composition identity of Gauss given in Theorem 2.2. Legendre [27] used the earlier identity (2b) in constructing his two-valued composite of weak form-classes. Perhaps what Bourbaki has in mind was this: Lagrange's identity (2d) may be regarded (and essentially was so regarded by Lagrange himself) as expressing the identity

$$Nm_{E/F}(xy) = (Nm_{E/F}x)(Nm_{E/F}y)$$

for quadratic field-extensions E/F, and in a sense this norm-identity explains the phenomenon of the existence of composition identities for binary quadratic forms. However, it was not until 1871 that an alternative definition of composition of proper form-classes was published, developed by Dedekind [18, Suppl. X] on the basis of this approach (this, at any rate, being the earliest such reference given in [15]).

(d) So far as the present author has been able to ascertain, (2d) and its derivation are the *only* contribution to the theory of composition of binary quadratic forms contained in the collected works of Lagrange (unless one wishes to include in this context certain relevant contributions by Lagrange to the general theory of binary quadratic forms over $\mathbb{Z}$, such as the concepts of discriminant and weak equivalence).

Actually, Definitions 2.2 and 2.3 do not do full justice to Gauss' original construction in [22], which we shall conclude this historical note by discussing. Let q and q' be binary quadratic forms of nonzero discriminant, and let Q be a Legendre composite of q and q' in the sense of Definition 2.1, i.e., let Q be transformed into the product of q and q' by the substitution given by a 2×4 unimodular matrix Σ. By Theorem 2.2, there exist rational numbers r and r' such that

$$q_\Sigma = rq, \quad q'_\Sigma = r'q', \quad Q_\Sigma = rr'Q.$$

In such a situation, Gauss then says [22, Art. 235] that Q is *composed* of q and q', *directly* or *inversely* of q (or of q') according as r (or r', respectively) is positive or negative. Also, in [22], when Gauss says simply that a form is composed of

two others, this is to be interpreted in Arts. 235–239 as meaning that it is a "Legendre composité" of the two others, in the sense of Def. 2.1, while from Art. 240 onwards this is rather to be interpreted as meaning that it is composed directly of each of the two others.

We shall here find it convenient to say that a form Q is an *extended Gaussian composite* of forms q and q' if Q is composed directly of q and directly of q'. This notion passes over to a binary operation on proper form-classes; if α and β are proper form-classes, the ratio of whose nonzero discriminants is the square of a rational number, then Gauss proved that the set of all extended Gaussian composites of a form in α with a form in β is a proper form-class, which Gauss called the composite of α and β, but which (to avoid conflict with Definition 2.3) will here be called the *extended composite* of α and β. Thus, Gauss' original construction achieves more than do Definitions 2.2 and 2.3; Gauss' construction applies to any pairs of forms of form-classes the ratio of whose nonzero discriminants is a perfect square, while Definitions 2.2 and 2.3 only apply to comaximal pairs which are of the same discriminant, and (if this discriminant is nonzero) they arise from Gauss' construction by restriction of the domain of definition.

There are several alternative ways to define the two concepts "Gaussian composite of two forms," "composite of two form-classes" besides the one given in this section. (For instance, there is the method of "united forms," due to Dirichlet and Dedekind: If α and α' are comaximal proper form-classes of the same discriminant, it may be proved that there exist integers a, a', b, c with

$$\text{g.c.d.}\quad (a, a', b) = 1,\ [a, b, a'c] \in \alpha,\ [a', b, ac] \in \alpha'$$

and then it follows from Example 7 that the composite $\alpha\beta$ is the class of $[aa', b, c]$.) At any rate, once these two concepts have been defined, it is easy to define directly in terms of them the two extended concepts of the preceding paragraph. Namely, given two binary quadratic forms q and q', the ratio of whose nonzero discriminants is the square of a rational number, it is easy to show there exist unique positive rational numbers r and r' such that rq and $r'q'$ are comaximal forms of the same discriminant; then Q is an extended Gaussian composite of q and q', if and only if $rr'Q$ is a Gaussian composite of rq and $r'q'$. For instance, since by Example 6, $[1, 1, 6]$ is a Gaussian composite of $[2, 1, 3]$ and $[2, -1, 3]$, it follows (with $r = \frac{1}{5}$, $r' = \frac{1}{2}$) that $[10, 10, 60]^L$ is an extended Gaussian composite of $[10, 5, 15]^L$ and $[4, -2, 6]^L$.

This extension of Definitions 2.2 and 2.3, though extremely simple once Definition 2.2 is available, seems too intimately connected with special properties of the ring $\mathbb{Z}$ to be suitable (as Definitions 2.2 and 2.3 are) for generalization to a wide class of rings; not only does this extension use the fact $\mathbb{Z}$ is a PID, but it also makes apparently essential use of the ordering on $\mathbb{Z}$. Note also that this extension is not needed for the definition of the Gaussian groups $G(\delta)$ (cf. Theorem 2.3).

In [9, pp. 163–166], Butts and Estes discuss, in this connection, possible substitutes over commutative domains for the requirement "r and r' are positive" in the preceding discussion; there seems to be no obvious natural condition generalizing this. A theory of extended composition over the ring $\mathbb{Z}[i]$ was given by Smith in [3, pp. 423–427]. Butts and Pall, in [10], discuss some number-theoretical applications of extended compsition over $\mathbb{Z}$.

It should be remarked that all binary quadratic forms considered by Gauss in [22] are required to have an even middle coefficient. This has no essential effect on the considerations of the present section, except that the set of groups $G(\delta)$ given by Theorem 2.3 properly contains the set of groups which arise working under this limitation.

Finally, note that if δ is negative, the composition groups $G(\delta)$ of Theorem 2.3 contain negative-definite as well as positive-definite form-classes. This is in conflict with the usual convention, which is to consider the subgroup $G_+(\delta)$ consisting of only the positive-definite form-classes in $G(\delta)$. However, $G(\delta)$ seems more suitable for generalization to larger classes of rings, and indeed, all the recent generalizations [8, 9, 25, 28] reduce to $G(\delta)$ when the ring is $\mathbb{Z}$. The relation between $G(\delta)$ and $G_+(\delta)$ is in any event a simple one: It is easy to show that $G(\delta)$ is the direct sum of its subgroup $G_+(\delta)$ and a subgroup isomorphic to $\mathbb{Z}_2$ (consisting of the identity element of $G(\delta)$ and its negative).

3. Forms of Type τ and R-Oriented $R\tau$-Modules

Throughout this section, R will denote a fixed ring on which 2 is not a zero-divisor; i.e., such that $2_R = 1_R + 1_R$ is not a zero-divisor in R. The objects of the binary operation "composition" to be defined in this section and the next are *oriented binary Lagrangian quadratic forms over* R and their form-classes; these will be referred to simply as "forms" and "form-classes."

Note that 2 is not a zero-divisor on R, if and only if, for every maximal ideal M of R, 2 is not a zero-divisor on R_M; note also that then 2_R is not a zero-divisor on any projective R-module P. An equation such as $q = \frac{1}{2}p$ (p and q in P) will then mean $2q = p$, and will be satisfied by a unique q if p is in $2P$.

Definition 3.1. By a *form-type* over R will be meant an ordered pair

$$\tau = (\delta, \pi)$$

in $R \times (R/2R)$ satisfying the conditions of Proposition 1.13, i.e., such that with Sq defined by

$$Sq\colon R/2R \to R/4R, \qquad r + 2R \mapsto r^2 + 4R$$

we have

$$Sq(\pi) = \delta + 4R. \tag{1}$$

A form (or form-class, or numerical L form) over R of discriminant δ and parity π will be said to be *of type* τ. The class of all forms of type τ, and the supclass consisting of all primitive such forms, are then both nonempty; we denote these classes by $F_R(\tau)$ and $PF_R(\tau)$, respectively. Similarly, we denote by $C_R(\tau)$ and $PC_R(\tau)$ the collection of all form-classes of type τ, and the collection of all primitive such form-classes, respectively.

The main purpose of the present paper is to define a binary operation, composition, on the forms in $PF_R(\tau)$, which passes over to a group operation on the form-classes in $PC_R(\tau)$. This operation will also be defined for certain comaximal pairs of forms in $F_R(\tau)$. In this section, we shall show that every form of type τ is associated with a module over a certain extension ring $R\tau$ of R; composition is then (partially) given by $\otimes_{R\tau}$.

If $\tau = (\delta, \pi)$ is a form-type over R and $f\colon R \to S$ is a ring-homomorphism, the form-type τ_f over S is well defined by

$$\tau = (\delta, b + 2R) \Rightarrow \tau_f = (f(\delta), f(b) + 2S)$$

and we then have maps

$$F_R(\tau) \to F_S(\tau_f), \qquad \gamma \mapsto \gamma_f, \tag{2a}$$

$$PF_R(\tau) \to PF_S(\tau_f), \qquad \gamma \mapsto \gamma_f, \tag{2b}$$

$$C_R(\tau) \to C_S(\tau_f), \qquad \operatorname{cls}\gamma \mapsto \operatorname{cls}\gamma_f, \tag{2c}$$

$$PC_R(\tau) \to PC_S(\tau_f), \qquad \operatorname{cls}\gamma \mapsto \operatorname{cls}\gamma_f \tag{2d}$$

induced by f (cf. Definition 1.8 and Lemma 1.11(ii)). In the special case when M is a prime ideal of R and f is the canonical map $R \to R_M$, we also denote τ_f by τ_M. Note that the form γ over R is of type τ, if and only if, for every maximal ideal M of R, γ_M is of type τ_M.

For the remainder of this section, $\tau = (\delta, \pi)$ *will denote a fixed form-type over* R. For every b in π, i.e., such that $b + 2R = \pi$, there is a unique $c(b)$ in R such that the numercial L form $[1, b, c(b)]^L$ is of type τ, i.e., such that $b^2 - 4c(b) = \delta$; by (1), and since 2 is not a zero-divisor on R, $c(b)$ is well defined by

$$c(b) = (b^2 - \delta)/4. \tag{3}$$

We now define $R(\tau, b)$ to be the ring

$$R(\tau, b) = R[X]/(X^2 + bX + c(b)) = R[\sigma_b] \tag{4}$$

with σ_b the residue class of X, and every element of R identified with its residue class. $R(\tau, b)$ does not essentially depend on the choice of representative b for the element π of $R/2R$; if also

$$b' = b + 2r \in \pi \qquad (r \text{ in } R),$$

then

$$f(b, b'): R(\tau, b) \to R(\tau, b'),\ r_1 + r_2\sigma_b \mapsto r_1 + r_2(\sigma_{b'} + r) \qquad (r_1 \text{ and } r_2 \text{ in } R) \quad (5)$$

is readily seen to be an R-algebra-isomorphism. We identity the various rings $R(\tau, b)$ by means of these isomorphisms, and denote the resulting ring by $R\tau$. Thus, (5) may now be written

$$\sigma_b = \sigma_{b'} + r \qquad \text{if} \quad b' = b + 2r \text{ with } r \text{ in } R. \tag{6}$$

(In more detail: (5) gives rise to an equivalence relation on the disjointified union of all $R(\tau, b)$ $(b \in \pi)$, and the elements of $R\tau$ are the equivalence classes with respect to this relation; σ_b now denotes the equivalence class containing the old σ_b ; we identify each element of R with its image in $R\tau$.)

$R\tau$ is free over R on 1 and σ_b ; hence, 2 is not a zero-divisor on $R\tau$. It follows from (6) that the rank 2 R-orientation

$$\epsilon_\tau = 1 \wedge \sigma_b \tag{7}$$

of $R\tau$ is independent of the choice of b in π. Similarly, (6) implies that the element $\langle \delta^{1/2} \rangle$ in $R\tau$ defined by

$$\langle \delta^{1/2} \rangle = b + 2\sigma_b \tag{8}$$

is independent of the choice of b in π. Clearly,

$$\sigma_b^2 + b\sigma_b + c(b) = 0, \tag{9}$$

whence $(\langle \delta^{1/2} \rangle)^2 = b^2 - 4c(b) = \delta$. It follows from (9) that if we define $\bar{\sigma}_b$ to be $-b - \sigma_b$, we have

$$X^2 + bX + c(b) = (X - \sigma_b)(X - \bar{\sigma}_b).$$

If b is in π and

$$s = r_1 + r_2\sigma_b \qquad (r_1 \text{ and } r_2 \text{ in } R)$$

is any element of $R\tau$, we define the *conjugate* $\bar{s}$ and *norm* Nms of s by

$$\begin{aligned} \bar{s} &= r_1 + r_2\bar{\sigma}_b = (r_1 - br_2) - r_2\sigma_b\,, \\ Nms &= s\bar{s} = r_1^2 - br_1r_2 + c(b)r_2^2. \end{aligned} \tag{10}$$

It is readily verified that these are independent of the choice of b in π, and that $s \to \bar{s}$ is an R-algebra-automorphism of $R\tau$, hence, that Nm is a multiplicative map from $R\tau$ into R, i.e.,

$$Nm(s_1 s_2) = (Nms_1)(Nms_2) \qquad (\text{all } s_1 , s_2 \text{ in } R).$$

(This is essentially Lagrange's identity, i.e., (2d) of Section 2.) In addition, Nm is a Lagrangian quadratic form on $R\tau$ over R and gives rise to the following important form of type τ.

DEFINITION 3.2. We denote by $\iota(\tau)$ the form $(R\tau, \epsilon_\tau , Nm)$.

Remarks. Here ϵ_τ is given by (7). It follows from (3) and (10) that $\iota(\tau)$ is in $PF_R(\tau)$. $\iota(\tau)$ will play the role of identity element for composition of forms of type τ.

Let us note the effect on the preceding constructions of a change of rings:

LEMMA 3.1. *Let S (as well as R) be a ring on which 2 is not a zero-divisor, and let $f: R \to S$ be a ring-homomorphism. There is then a unique ring-homomorphism*

$$\tilde{f}_\tau : R\tau \to S\tau_f$$

such that

$$\tilde{f}_\tau(r_1 + r_2\sigma_b) = f(r_1) + f(r_2)\sigma_{f(b)} \qquad (\textit{for all } r_1 \textit{ and } r_2 \textit{ in } R,\ b \textit{ in } \pi). \tag{11}$$

$\tilde{f}_\tau$ restricted to R is f, and for every s in $R\tau$, $\tilde{f}_\tau(s)$ has conjugate $\tilde{f}_\tau(\bar{s})$ and norm $f(Nms)$.

There is a natural S-algebra-isomorphism

$$f_\tau : (R\tau)_f \to S\tau_f , \ s_f \mapsto \tilde{f}_\tau(s) \qquad (s \textit{ in } R\tau) \tag{12}$$

which is, moreover, a proper equivalence over S from $(\iota(\tau))_f$ to $\iota(\tau_f)$, and maps $(\langle \delta^{1/2} \rangle)_f$ into $\langle \delta_f^{1/2} \rangle$.

Proof. Straightforward.

The assertions made in the course of the following key definition are justified below in Proposition 3.2.

DEFINITION 3.3. *Let $\gamma = (P, \epsilon, q)$ be a form of type τ. There exists a unique R-endomorphism $T(\gamma)$ of P such that*

$$p_1 \wedge (T(\gamma)p_2) = B_q(p_1 \otimes p_2)\epsilon \qquad (\text{all } p_1 \textit{ and } p_2 \text{ in } P). \tag{13}$$

For b in π,

$$T_b(\gamma) = \tfrac{1}{2}(T(\gamma) - b\,\mathrm{Id}_P)$$

defines an R-endomorphism of P (i.e. $T(\gamma) - b\,\mathrm{Id}_P$ maps P into $2P$). We may define on P the structure of an $R\tau$-module by letting $T_b(\gamma)$ be multiplication by σ_b on P, i.e., by the formula

$$(r_1 + r_2\sigma_b)p = r_1p + r_2T_b(\gamma)p \qquad (r_1 \text{ and } r_2 \text{ in } R,\ p \text{ in } P).$$

This $R\tau$-module (which is independent of the choice of b in π) will be denoted by P_γ.

EXAMPLE. Suppose R is the field $\mathbb{R}$ of real numbers, $P = \mathbb{R}^2$, $\epsilon = \binom{1}{0} \wedge \binom{0}{1}$ and q is the Euclidean metric $\binom{x}{y} \mapsto x^2 + y^2$. Here $R/2R$ is the zero ring, $\delta = -4$. We may take $b = 0$, $c(b) = 1$; then

$$\mathbb{R}\tau = \mathbb{R}[X]/(X^2 + 1) = \mathbb{C},\ \sigma_0 = 1.$$

It is readily seen, using the equations

$${}^t(x_1, x_2) \wedge {}^t(y_1, y_2) = (x_1y_2 - x_2y_1)\epsilon$$

$$B_q({}^\tau(x_1, x_2) \otimes {}^t(y_1, y_2)) = (x_1 + y_1)^2 + (x_2 + y_2)^2 - (x_1^2 + x_2^2) - (y_1^2 + y_2^2) = 2(x_1y_1 + x_2y_2)$$

that (13) has the unique solution

$$T(\gamma){}^t(y_1, y_2) = {}^t(-2y_2, 2y_1)$$

whence $\mathbb{R}^2$ is given the $\mathbb{C}$-module structure

$$i{}^t(y_1, y_2) = T_0(\gamma){}^t(y_1, y_2) = {}^t(-y_2, y_1).$$

This is exactly the usual C-module structure on $\mathbb{R}^2$ associated with the Argand diagram, in which ${}^t(y_1, y_2)$ is identified with $y_1 + iy_2$. Note the role played by the orientation ϵ; if we were only given a two-dimensional Euclidean space (P, q), it would be impossible uniquely to specify multiplication by σ_0 as a *counterclockwise* rotation by a right angle.

Remark. The motivation for Definition 3.3 was as follows: Suppose P is free, say on $\{e_1, e_2\}$ with $e_1 \wedge e_2 = \epsilon$; there are then a', b', c' in R with

$$q(xe_1 + ye_2) = a'x^2 + b'xy + c'y^2 \qquad (\text{all } x, y \text{ in } R).$$

We wish to extend the given R-module structure on P to an R_τ-module structure, i.e., to define an R-homomorphism

$$\psi\colon R_\tau \otimes_R P \to P, \qquad s \otimes p \mapsto sp.$$

Consider the L-quadratic forms over R,

$$\begin{aligned} Nm\colon x + y\sigma_b &\mapsto x^2 - bxy + c(b)y^2 \quad \text{on} \quad R_\tau, \\ q\colon xe_1 + ye_2 &\mapsto a'x^2 + b'xy + c'y^2 \quad \text{on} \quad P. \end{aligned}$$

We have the composition identity (transforming q into $(Nm)\,(q)$)

$$(x^2 - bxy + c(b)y^2)(a'x'^2 + b'x'y' + c'y'^2) = a'X^2 + b'XY + c'Y^2$$

with

$$\begin{aligned} X &= xx' - \tfrac{1}{2}(b + b')yx' - c'yy', \\ Y &= xy' + a'yx' + \tfrac{1}{2}(b' - b)yy'. \end{aligned}$$

(Recall that $b' + 2R = b + 2R = \pi$.) This suggests as a distinguished candidate for ψ the R-homomorphism

$$(x + y\sigma) \otimes (x'e_1 + y'e_2) \to Xe_1 + Ye_2$$

and Definition 3.3 was obtained by concocting an equivalent basis-free way of stating this choice for ψ (cf. also Proposition 3.2, Corollary 3 below).

PROPOSITION 3.2. *Let $\gamma = (P, g, q)$ lie in $F_R(\tau)$. The G-quadratic form B_q on P over R induces an R-homomorphism*

$$\mu_q : P \to P^*,\ p_1 \mapsto (p_2 \mapsto B_q(p_1 \otimes p_2)).$$

With λ_ϵ denoting the R-isomorphism $P \to P^*$ of Definition 1.7, *let*

$$T(\gamma) = -\lambda_\epsilon^{-1} \circ \mu_q\,; \tag{14}$$

then $T(\gamma)$ is the unique R-homomorphism $P \to P$ satisfying (13). *If b is in π, $T(\gamma) - b\,\mathrm{Id}_P$ maps P into $2P$; since 2_R is not a zero-divisor on P, there is thus a unique R-homomorphism $T_b(\gamma)\colon P \to P$ such that*

$$2T_b(\gamma) = T(\gamma) - b\,\mathrm{Id}_P \tag{15}$$

and $T_b(\gamma)$ then satisfies

$$[T_b(\gamma)]^2 + bT_b(\gamma) + c(b)\,\mathrm{Id}_P = 0.$$

Proof. First verifying that μ_q and λ_ϵ, and so $T(\gamma)$ as defined by (14), behave well under localization (cf. Lemma 1.7), we may employ the usual localization argument to reduce to the case when P is free over R. Thus, we may now assume: *P is free over R on $\{e_1, e_2\}$, and for some a', b', and c' in R,*

$$e_1 \wedge e_2 = \epsilon,\ q(x_1e_1 + x_2e_2) = a'x_1^2 + b'x_1x_2 + c'x_2^2 \text{ for all } x_1 \text{ and } x_2 \text{ in } R. \quad (16)$$

Let $\{e_1^*, e_2^*\}$ be the dual basis for P^* and suppose that

$$p_1 = x_1e_1 + x_2e_2,\ p_2 = y_1e_1 + y_2e_2 \qquad (x_i \text{ and } y_i \text{ in } R).$$

Then

$$p_1 \wedge p_2 = (x_1y_2 - x_2y_1)\epsilon, \quad (17)$$

$$\lambda_\epsilon(p_1) = -x_2e_1^* + x_1e_2^*, \quad (18)$$

$$B_q(p_1 \otimes p_2) = 2a'x_1y_1 + b'(x_1y_2 + x_2y_1) + 2c'x_2y_2 \quad (19)$$

(using Eq. (19) of Section 1) whence

$$\mu_q(p_1) = (2a'x_1 + b'x_2)e_1^* + (b'x_1 + 2c'x_2)e_2^*, \quad (20)$$

$$T(\gamma)p_1 = -(b'x_1 + 2c'x_2)e_1 + (2a'x_1 + b'x_2)e_2\,. \quad (21)$$

Using these formulas, we readily verify that $T(\gamma) = -\lambda_\epsilon^{-1} \circ \mu_q$ is the unique solution to (13). Since

$$b' + 2R = \pi(\gamma) = \pi = b + 2R, \qquad \text{i.e.,}\quad b \equiv b' \pmod{2R},$$

it follows that $(T(\gamma) - b\,\mathrm{Id}_P)p_1$ is in $2P$, and is twice the following element of P:

$$T_b(\gamma)p_1 = -(\tfrac{1}{2}(b' + b)x_1 + c'x_2)e_1 + (a'x_1 + \tfrac{1}{2}(b' - b)x_2)e_2\,. \quad (22)$$

$T_b(\gamma)$ is thus represented with respect to the free basis $\{e_1, e_2\}$ for P by the matrix

$$M = \begin{pmatrix} -\frac{1}{2}(b + b'), & -c' \\ a', & \frac{1}{2}(b' - b) \end{pmatrix}$$

It is readily verified that

$$M^2 + bM + c(b)I_2 = [\tfrac{1}{4}(b'^2 - b^2) - a'c' + c(b)]I_2$$

which is 0 since

$$b'^2 - 4a'c' = \delta = b^2 - 4c(b).$$

Hence,

$$[T_b(\gamma)]^2 + bT_b(\gamma) + c(b)\,\mathrm{Id}_P = 0.$$

COROLLARY 1. *Let the free form $\gamma = (P, \epsilon, q)$ over R of type $\tau = (\delta, \pi)$ be represented by $[a', b', c']^L$ with respect to the properly oriented free basis $\{e_1, e_2\}$ (cf. Definition* 1.10*) and let $b \in \pi$; then*

$$\sigma_b(x_1e_1 + x_2e_2) = -[\tfrac{1}{2}(b' + b)x_1 + cx_2]e_1 + [ax_1 + \tfrac{1}{2}(b' - b)x_2]e_2\,,$$

i.e.,

$$\sigma_b e_1 = -\tfrac{1}{2}(b' + b)e_1 + ae_2\,, \qquad \sigma_b e_2 = ce_1 + \tfrac{1}{2}(b' - b)e_2\,.$$

Proof. This is just 22), which was proved under exactly these hypotheses.

COROLLARY 2. *The $R\tau$-module structure $(R\tau)_{\iota(\tau)}$ on $R\tau$ associated with the form*

$$\iota(\tau) = (R\tau,\ 1 \wedge \sigma_b\,,\ Nm)$$

of Definition 3.2 *is the usual one (i.e., the module product $s_1 \cdot s$ is the ring product).*

Proof. By (10), (16) holds with

$$e_1 = 1, \quad e_2 = \sigma_b\,, \quad a' = 1, \quad b' = -b, \quad c' = c(b).$$

Applying (9) and (22) we obtain

$$T_b(\iota(\tau))(x_1 + x_2\sigma_b) = -c(b)x_2 + (x_1 - bx_2)\sigma_b = \sigma_b(x_1 + x_2\sigma_b),$$

i.e., the multiplication $T_b(\iota(\tau))$ by σ_b on the $R\tau$-module $(R\tau)_{\iota(\tau)}$ coincides with the multiplication by σ_b in the ring $R\tau$.

COROLLARY 3. *Let $\gamma = (P, \epsilon, q)$ be a form of type τ; then*

$$q(sp) = (Nms)q(p) \qquad (\textit{all } s \textit{ in } R\tau,\ p \textit{ in } P)$$

(the product sp being taken in the sense of the $R\tau$-module P_γ).

Proof. Using the method of localization, we may assume that P is free over R on $\{e_1, e_2\}$ and that (16) holds. If

$$q = x + y\sigma_b\,, \ p = x'e_1 + y'e_2 \qquad (x, y, x', y' \text{ in } R),$$

then using (22) we see that $qp = Xe_1 + Ye_2$ with

$$X = xx' - \tfrac{1}{2}(b + b')yx' - c'yy',$$
$$Y = xy' + a'yx' + \tfrac{1}{2}(b' - b)yy'$$

and we must then prove that

$$a'X^2 + b'XY + c'Y^2 = (x^2 - bxy + c(b)y^2)(a'x'^2 + b'x'y' + c'y'^2).$$

This follows from Gauss' Composition identity (Proposition 2.4) applied to the 2×4 matrix

$$\Sigma = \begin{pmatrix} 1, & 0, & -\frac{1}{2}(b + b'), & -c' \\ 0, & 1, & a', & \frac{1}{2}(b' - b) \end{pmatrix}$$

over R (also using the fact that $b'^2 - 4a'c' = \delta = b^2 - 4c(b)$.

LEMMA 3.3. *Let $\gamma = (P, \epsilon, q)$ be a form of type τ over R.*

(i) *If T is a proper R-equivalence from γ to $\gamma' = (P', \epsilon', q')$, then $T: P_\gamma \mapsto (P')_{\gamma'}$ is an $R\tau$-isomorphism.*

(ii) *Let $f: R \to S$ be a ring-homomorphism and assume 2 is also not a zero-divisor on S. (cf. Lemma 3.1 for the meaning of $\tilde{f}_\tau$ and f_τ)*

$$[T_b(\gamma)]_f = T_{f(b)}(\gamma_f),$$

or equivalently,

$$(\sigma p)_f = \tilde{f}_\tau(\sigma)p_f \qquad (\sigma \text{ in } R\tau,\ p \text{ in } P).$$

This conclusion may also be stated in the following form: the identity map on P_f is a f_τ-homomorphism from the $(R\tau)_f$-module $(P_\gamma)_f$ to the $S\tau_f$-module $(P_f)_{\gamma_f}$.

Proof. Straightforward.

We next examine the conditions for an $R\tau$-module to be of the form P_γ. These results will not be used in Section 4 of the present paper.

DEFINITION 3.4. Let R be a subring of S (with $1_R \equiv 1_S$). By a *rank n R-oriented S-module* will be meant an ordered pair (P, ϵ) where P is an S-module which, when considered as an R-module, has the rank n R-orientation ϵ; we then say P is a *rank n R-orientable S-module.* If (P, ϵ) and (P', ϵ') are two rank n R-oriented S-modules, a map $T: P \to P'$ will be called an *R-oriented S-isomorphism* if T is both an S-isomorphism and an R-oriented R-isomorphism.

DEFINITION 3.5. A rank 2 R-orientable $R\tau$-module P (or a rank 2 R-oriented $R\tau$-module (P, ϵ)) will be called *compatible* if for one (and hence all) b in π the R-endomorphism

$$\sigma_b(P): P \to P,\ p \mapsto \sigma_b p$$

has characteristic polynomial $X^2 + bX + c(b)$ over R (cf. Eq. (3) and Definition 1.7), i.e., has the same characteristic polynomial over R as $\sigma_b(R\tau)$.

LEMMA 2.4. *Let $f: R \to S$ be a ring-homomorphism, S a ring on which 2 is not a zero-divisor, P a compatible R-orientable $R\tau$-module; then P_f is a compatible S-orientable $S\tau_f$-module. An R-orientable $R\tau$-module P is compatible, if and only if, for every maximal ideal M of R, the R_M-orientable $R_M\tau_M$-module, P_M is compatible.*

Proof. Straightforward.

PROPOSITION 3.5. (a) *If $\gamma = (P, \epsilon, q)$ is in $F_R(\tau)$, then (P_γ, ϵ) is a compatible rank 2 R-oriented $R\tau$-module.*

(b) *Let b lie in π. A rank 2 R-orientable $R\tau$-module P is compatible if and only if $\mathrm{tr}_R\, \sigma_b(P) - b$.*

(c) *A rank 2 R-orientable $R\tau$-module P is compatible if P is a faithful $R\tau$-module (i.e., if no nonzero element of $R\tau$ annihilates P).*

Proof. Using Lemma 2.4, we may reduce by localization to the case:

$$P \text{ is free over } R \text{ on } \{e_1, e_2\}.$$

Let b lie in π.

(Ad a) We may assume $e_1 \wedge e_2 = \epsilon$. For some a', b', and c' in R,

$$q(x_1e_1 + x_2e_2) = a'x_1^2 + b'x_1x_2 + c'x_2^2 \qquad (\text{all } x_1, x_2 \text{ in } R)$$

and, therefore, $b'^2 - 4a'c' = b^2 - 4c(b)$, $b \equiv b' \pmod{2R}$. By Definition 3.3, $\sigma_b(P_\gamma) = T_b(\gamma)$, which was seen (under the present hypotheses) in the proof of Proposition 3.2 to be represented with respect to the free basis $\{e_1, e_2\}$ over R by the matrix

$$\begin{pmatrix} -\frac{1}{2}(b' + b), & -c' \\ a' & \frac{1}{2}(b' - b) \end{pmatrix}$$

This matrix has trace $-b$ and determinant

$$\tfrac{1}{4}(b^2 - b'^2) + a'c' = \tfrac{1}{4}(b^2 - (b'^2 - 4a'c')) = \tfrac{1}{4}[b^2 - (b^2 - 4c(b))] = c(b)$$

and, hence, characteristic polynomial $X^2 + bX + c(b)$; hence, so does $\sigma_b(P_\gamma)$ over R.

(Ad b) $\chi_R(\sigma_b(P)(X) = X^2 - (\mathrm{tr}_R\, \sigma_b(P))X + \det_R \sigma_b(P)$, by Proposition 1.6, so it suffices to show

$$\mathrm{tr}_R \sigma_b(P) = -b \Rightarrow \det_R \sigma_b(P) = c(b).$$

Suppose $\sigma_b(P)$ is represented with respect to the free basis $\{e_1, e_2\}$ by the matrix

$$\begin{pmatrix} s_1, & s_2 \\ t_1, & t_2 \end{pmatrix}$$

over R. Equation (9) implies that $[\sigma_b(P)]^2 + b\sigma_b(P) + c(b\ \mathrm{Id}_P = 0$, so

$$\begin{pmatrix} s_1, & s_2 \\ t_1, & t_2 \end{pmatrix}^2 + b \begin{pmatrix} s_1, & s_2 \\ t_1, & t_2 \end{pmatrix} + c(b) \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \quad \begin{pmatrix} 0, & 0 \\ 0, & 0 \end{pmatrix}$$

and, therefore, (equating the upper left-hand entries of both sides of the preceding equation)

$$s_1^2 + s_2 t_1 + b s_1 + c(b) = 0.$$

Hence, if

$$\mathrm{tr}_R\, \sigma_b(P) = s_1 + t_2 = -b,$$

then

$$-c(b) = s_1^2 + s_2 t_1 + (-s_1 - t_2)s_1 = s_2 t_1 - s_1 t_2\,,$$

i.e., $c(b) = \det_R \sigma_b(P)$.

(Ad c) As was just noted,

$$[\sigma_b(P)]^2 + b\sigma_b(P) + c(b)\,\mathrm{Id}_P = 0$$

while by Proposition 1.6,

$$[\sigma_b(P)]^2 - [\mathrm{tr}_R\, \sigma_b(P)]\sigma_b(P) + [\det_R \sigma_b(P)]\,\mathrm{Id}_P = 0.$$

Hence,

$$[b + \mathrm{tr}_R\, \sigma_b(P)]\sigma_b(P) + [c(b) - \det_R \sigma_b(P)]\,\mathrm{Id}_P = 0,$$

i.e.,

$$[(b + \mathrm{tr}_R\, \sigma_b(P))\sigma_b + (c(b) - \det_R \sigma_b(P)]p = 0 \qquad (\text{all } p \text{ in } P).$$

Hence, if P is a faithful R_T-module,

$$b + \mathrm{tr}_R\, \sigma_b(P) = c(b) - \det_R \sigma_b(P) = 0$$

so P is compatible.

COROLLARY. *If P is a rank 2 R-orientable invertible R_T-module, then P is compatible.*

Proof. P is locally R_T-isomorphic to R_T, hence, faithful over R_T.

The following counterexamples show directions in which Proposition 3.5 cannot be immediately strengthened.

EXAMPLE 1. This example shows not every rank 2 R-orientable $R\tau$-module is compatible: $R = \mathbb{Z}$, $\tau = (4, 2Z)$, $P = \mathbb{Z}^2$ with P given the structure of a module over $R\tau$ by the equation

$$(m + n\sigma_0)p = (m + n)p \qquad (m \text{ and } n \text{ in } \mathbb{Z},\ p \text{ in } \mathbb{Z}^2).$$

Note that (with $b = 0$) $\operatorname{tr}_R \sigma_b(P) = 2 \neq -b$; thus, P is not compatible.

EXAMPLE 2. Another example, which is not compatible even though $\sigma_b(P)$ has the "correct" determinant $c(b)$ over R: $R = \mathbb{Z}_9$, $\tau = (0, 2\mathbb{Z}_9)$, $P = (\mathbb{Z}_9)^2$, with an $R\tau$-module structure on P given by $\sigma_0 p = 3p$ (all p in P).

EXAMPLE 3. $R = \mathbb{Z}_{15}$, $\gamma = (P, \epsilon, q)$ with $P = (\mathbb{Z}_{15})^2$, $\epsilon = \binom{1}{0} \wedge \binom{0}{1}$ and

$$q\left(\binom{x}{y}\right) = 3x^2 + 3y^2.$$

Here $\delta = \{9\}$, $R/2R$ is the zero ring; we may pick b to be 0, and then multiplication by σ_0 on P_γ is given by the matrix

$$\begin{pmatrix} \{0\}, & -\{3\} \\ \{3\}, & \{0\} \end{pmatrix}$$

so that $5\sigma_0$ annihilates P. Thus, the compatible module P_γ is not faitful.

PROPOSITION 3.6. *Let $FOr_R(\tau)$ denote the class of all compatible rank 2 R-oriented $R\tau$-modules; then the map*

$$\theta(\tau)\colon F_R(\tau) \to FOr_R(\tau),\ \gamma = (P, \epsilon, q) \mapsto (P_\gamma, \epsilon)$$

is a bijection.

Proof. We construct an inverse map

$$\psi\colon FOr_R(\tau) \to F_R(\tau)$$

to θ as follows. Let (P, ϵ) be a compatible rank 2 R-oriented $R\tau$-module. Motivated by Eq. (13) (with $T_b(\gamma)$ multiplication by σ_b and $T(\gamma) = 2T_b(\gamma) + b\,\mathrm{Id}_P$ multiplication by $b + 2\sigma_b$) we define (for any b in π)

$$B(P, \epsilon) = B\colon P \otimes_R P \to R$$

by

$$B(p_1 \otimes p_2)\epsilon = p_1 \wedge ((b + 2\sigma_b)p_2) \qquad (\text{all } p_1 \text{ and } p_2 \text{ in } P). \tag{23}$$

To prove that θ is a bijection, it will suffice to prove the following statement:

(a) B, as defined by (23), is a Gaussian quadratic form on P over R;

(b) *The associated L quadratic form q_B on P over R (cf. Definition* 1.3) *maps P into $2R$;*

(c) *The form*

$$\psi(P, \epsilon) = (P, \epsilon, \tfrac{1}{2}q_{B(P,\epsilon)}) \tag{24}$$

is of type τ.

Namely, these being proved, we have available the map ψ given by (24), which is easily verified to be inverse to θ.

The statements (a), (b), and (c) localize well; thus, it suffices to prove than under the additional assumption:

$$P \text{ is free over } R \text{ on } \{e_1, e_2\} \text{ with } e_1 \wedge e_2 = \epsilon.$$

Let be lie in π. There are then elements s_1, s_2, t_1, t_2 in R with

$$\sigma_b e_1 = s_1 e_1 + s_2 e_2, \qquad \sigma_b e_2 = t_1 e_1 + t_2 e_2. \tag{25}$$

Suppose

$$p_1 = x_1 e_1 + x_2 e_2, \qquad p_2 = y_1 e_1 + y_2 e_2,$$

then it readily follows from (23) and (25) that

$$B(p_1 \otimes p_2) = 2s_2 x_1 y_1 + (2t_2 + b)x_1 y_2 - (2s_1 + b)x_2 y_1 - 2t_1 x_2 y_2. \tag{26}$$

To prove (a), i.e., to show that

$$2t_2 + b = -(2s_1 + b) \tag{27}$$

it suffices to note that, P being by hypothesis compatible, the matrix

$$\begin{pmatrix} s_1, & s_2 \\ t_1, & t_2 \end{pmatrix}$$

representing $\sigma_b(P)$ with respect to the free basis $\{e_1, e_2\}$, has trace $-b$ and determinant $c(b)$, i.e.,

$$s_1 + t_2 = -b, \qquad s_1 t_2 - s_2 t_1 = c(b) \tag{28}$$

which clearly implies (27). Noting also that thus, both sides of (27) equal $t_2 - s_1$, we have

$$B(p_1 \otimes p_2) = 2s_2 x_1 y_1 + (t_2 - s_1)(x_1 y_2 + x_2 y_1) - 2t_1 x_2 y_2$$

which immediately yields (b) and the formula

$$q(p_1) = s_2x_1^2 + (t_2 - s_1)x_1x_2 - t_1x_2^2$$

for $q = \frac{1}{2}q_{B(P,\epsilon)}$. Finally, (c) follows from the facts that (using (3) and (28))

$$\delta(q) = (t_2 - s_1)^2 + 4s_2t_1 = (t_2 + s_1)^2 - 4(s_1t_2 - s_2t_1) = b^2 - 4c(b) = \delta,$$
$$\pi(q) = t_2 - s_1 + 2R = t_2 + s_1 + 2R = b + 2R = \pi.$$

PROPOSITION 3.7. *The map $\theta(\tau)$ of Proposition* 3.6 *is an isomorphism from the category of forms of type τ over R and natural equivalences over R into the category of compatible rank* 2 *R-oriented $R\tau$-modules and R-oriented $R\tau$-isomorphisms. $\theta(\tau)$ is natural in R in the following sense*:

Let $f\colon R \to S$ be a ring-homomorphism, and suppose 2 *is not a zero-divisor on S. Then there is a commutative diagram*

$$\begin{array}{ccc} F_R(\tau) & \xrightarrow{\alpha} & F_S(\tau_f) \\ {\scriptstyle\theta(\tau)}\downarrow & & \downarrow{\scriptstyle\theta(\tau_f)} \\ FOr_R(\tau) & \xrightarrow{\beta} & FOr_S(\tau_f) \end{array}$$

where α is the map in (2a) *and β is defined in terms of the map $\tilde{f}_\tau$ given by* (11) *as follows* (*cf. Lemma* (3.3)):

$$\beta(P, \epsilon) = (P_{(\tilde{f}_\tau)}, \epsilon_f).$$

Proof. Straightforward.

4. Composition of Forms and Form-Classes over Rings

Throughout this section, as in Section 3 "form" and "form-class" will mean "oriented binary Lagrangian quadratic form" and "proper binary Lagrangian quadratic form-class," respectively; also, R will denote a ring on which 2 is not a zero-divisor. We shall denote by cls γ the form-class over R containing a given form γ over R.

DEFINITION 4.1. Let

$$\gamma = (P, \epsilon, q),\ \gamma' = (P', \epsilon', q')$$

be two forms over R of the same type τ; then the form

$$\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q})$$

over R will be called a *semi-composite* of γ and γ' if it satisfies the following three conditions:

(i) $\bar{\gamma}$ is of type τ.

(ii) The $R\tau$-module $\bar{P}_{\bar{\gamma}}$ (cf. Definition 3.3) coincides with $P_\gamma \otimes_{R\tau} P'_{\gamma'}$.

(iii) For all p ib P and p' in P', the element $p \otimes_{R\tau} p'$, which lies in $P_\gamma \otimes_{R\tau} p'_{\gamma'}$, and hence by (ii) in $\bar{P}$, satisfies

$$\bar{q}(p \otimes_{R\tau} p') = q(p)\, q'(p'). \tag{1}$$

If γ and γ' have a unique semi-composite, it will be called their *composite*; in this case, we say that γ and γ' are *composable*, and denote their composite by $\gamma\gamma'$.

Let $\tau = (\delta, \pi)$; then it turns out that the notions "semi-composite" and "composite" coincide except possibly when the forms are not primitive, and δ, the common discriminant of the two forms being composed, is a zero-divisor in R. This matter will be clarified in Theorem 4.8 and its corollaries.

Note that under this definition *forms* are composed, not merely *form-classes*. The construction of Gauss described in Section 2 (and its generalization in [8, 9]) does not assign a unique composite to two numerical forms, a binary operation only being obtained after passing to proper form-classes; the same is true of the two other classical composition constructions, that of Dirichlet–Dedekind via "united forms," and that of Dedekind via multiplication of narrow ideal-classes in quadratic number-fields. It is this feature of the present construction, a feature very likely unattainable in any natural way so long as we restrict ourselves to numerical rather than oriented forms over R, which makes possible the existence proof in Theorem 4.11 below, which constructs a composite of two forms over R by piecing together their composite in each localization R_M. (If we were obliged to work with form-classes, upon returning to the global situation we would come up with at best an equivalence class of forms under a grosser relation of "local equivalence over R," with not even a guarantee of being able to piece the local composites together; the difference is that the forms constitute a sheaf over Spec R, and the form-classes do not.)

Let us note the following consequences of condition (iii) in Definition 4.1. If p_1 and p_2 are in P, p' in P', then the "composition identity" (1) implies

$$\bar{q}((p_1 + p_2) \otimes_{R\tau} p') = q(p_1 + p_2)\, q'(p'),\ \bar{q}(p_i \otimes_{R\tau} p') = q(p_i)\, q'(p') \qquad (i = 1, 2)$$

whence (cf. Definition 1.3 for the meaning of B_q)

$$B_{\bar{q}}(p_1 \otimes_{R\tau} p', p_2 \otimes_{R\tau} p') = B_q(p_1, p_2)\, q'(p'). \tag{1a}$$

Similarly,

$$B_{\bar{q}}(p \otimes_{R\tau} p'_1, p \otimes_{R\tau} p'_2) = q(p)\, B_{q'}(p'_1, p'_2) \tag{1b}$$

for all p in P, p_1', p_2' in P'; a further polarization yields

$$B\mathrm{f}(p_1, p_2)\, B_{q'}(p_1', p_2') = B_{\bar{q}}(p_1 \otimes_{R\tau} p_1', p_2 \otimes_{R\tau} p_2') + B_{\bar{q}}(p_1 \otimes_{R\tau} p_2', p_2 \otimes_{R\tau} p_1') \tag{1c}$$

for all p_1, p_2 in P and p_1', p_2' in P'.

THEOREM 4.1. *Let R and S be rings on which 2 is not a zero-divisor, and let $f\colon R \to S$ be a ring-homomorphism. Let the form $\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q})$ over R be a semi-composite of the two forms*

$$\gamma = (P, \epsilon, q) \qquad \text{and} \qquad \gamma' = (P', \epsilon', q')$$

over R. Then there exists a proper S-equivalence ψ from $\bar{\gamma}_f$ to a semicomposite of γ_f and γ_f', namely, the natural S-isomorphism

$$\psi\colon (P_\gamma \otimes_{R\tau} P'_{\gamma'})_f \to (P_f)_{\gamma_f} \otimes_{S\tau_f} (P'_f)_{\gamma'_f}, \tag{2}$$

$$(p \otimes_{R\tau} p')_f \mapsto p_f \otimes_{S\tau_f} p'_f \qquad (p \text{ in } P,\ p' \text{ in } P').$$

Proof. In the course of demonstrating this theorem, the following notation will temporarily be adopted to avoid ambiguity:

Ordinarily, $\phi\colon R_1 \to R_2$ being a ring-homomorphism, one says that a map g from a R_1-module E_1 to a R_2-module E_2 is a ϕ-homomorphism if

$$g(e + e') = g(e) + g(e'),\ g(re) = \phi(r)\, g(e) \qquad (\text{all } e \text{ and } e' \text{ in } E_1,\ r \text{ in } R_1).$$

Because, in establishing (ii) of Definition 4.1, we shall have to consider "two" module structures (not yet proved coincident) on the same set, we shall need to be unusually careful and attribute the property of being a ϕ-homomorphism to the ordered triple (g, E_1, E_2) rather than to the mere map g. In the course of the present proof, an ordered triple such as (under the preceding assumptions) (g, E_1, E_2) will be called: *g considered as a map from the R_1-module E_1 to the R_2-module E_2*, and will be denoted by $g\colon E_1 \nrightarrow E_1$; g will be called the *underlying map* of this triple, and the triple will be called *bijective* when g is. (The point is this: If E_2' is a second R_2-module with the same underlying set as E_2, $g\colon E_1 \nrightarrow E_2'$ need not be a ϕ-homomorphism even though it has the same underlying map g as the ϕ-homomorphism $g\colon E_1 \nrightarrow E_2$.)

By the corollary to Lemma 1.4, there is a natural $(R\tau)_f$-isomorphism

$$\psi_1 : (P_\gamma \otimes_{R\tau} P'_{\gamma'})_f \to (P_\gamma)_f \otimes_{(R\tau)_f} (P'_{\gamma'})_f,$$

$$(p \otimes_{R\tau} p')_f \mapsto p_f \otimes_{(R\tau)_f} p'_f.$$

Lemma 3.1 yields the S-algebra isomorphism f_τ: $(R\tau)_f \approx R\tau_f$, and by Lemma 3.3 there is then an f_τ-homomorphism

$$\psi_2 : (P_\gamma)_f \otimes_{)R\tau)_f} (P'_{\gamma'}) \to (P_f)_{\gamma_f} \otimes_{S\tau_f} (P'_\gamma)_{f'_f},$$

$$p_f \otimes_{(R\tau)_f} p'_f \mapsto p_f \otimes_{S\tau_f} p'_f .$$

The composite $\psi_2 \circ \psi_1$ of the underlying maps is exactly the map ψ of (2); thus,

$$\psi: (P_\gamma \otimes_{R\tau} P'_{\gamma'})_f \to (P_f)_{\gamma_f} \otimes_{S\tau_f} (P'_f)_{\gamma'_f}$$

is a bijective f_τ-homomorphism, and in particular, its underlying map ψ is an S-isomorphism, considered as a map of the underlying S-modules.

By (ii) of Definition 4.1, $\bar{P}$ is the R-module underlying the R-module $P_\gamma \otimes_R P'_{\gamma'}$; thus, the domain of ψ is $\bar{P}_f$, so that $\psi_*\bar{\gamma}_f$ makes sense (cf. Definition 1.10). The theorem to be proved essentially asserts that $\psi_*\bar{\gamma}_f$ is a semi-composite of γ_f and γ'_f (cf. Proposition 1.8); we now prove this by verifying that these three forms satisfy (i), (ii), and (iii) of Definition 4.1.

(Ad (i) $\bar{\gamma}$ is of the same type τ as γ and γ', by Definition 4.1(i). Hence, γ_f, γ'_f, $\bar{\gamma}_f$ are of type τ_f (by Lemma 1.11(ii)), as is $\sigma_*\bar{\gamma}_f$ (by Lemma 1.11(i)).

(Ad (ii) Let $\psi_*\bar{\gamma}_f = \tilde{\gamma} = (\tilde{P}, \tilde{\epsilon}, \tilde{q})$. We must prove the following statement:

(A) *The $S\tau_f$-modules $\tilde{P}_{\tilde{\gamma}}$ and $(P_f)_{\gamma_f} \otimes_{S\tau_f} (P'_f)_{\gamma'_f}$ coincide.*

Since $\bar{\gamma}$ is a semi-composite of γ and γ', $\bar{P}_{\bar{\gamma}} = P_\gamma \otimes_{R\tau} P'_{\gamma'}$, and the following statement then follows from our earlier discussion of ψ:

(B) $\psi: (\bar{P}_{\bar{\gamma}})_f \to (P_f)_{\gamma_f} \otimes_{S\tau_f} (P'_f)_{\gamma'_f}$ *is a bijective f_τ-homomorphism.*

$\tilde{P} = \psi(\bar{P}_f)$ is the S-module underlying the $S\tau_f$-module $(P_f)_{\gamma_f} \otimes_{S\tau_f} (P'_f)_{\gamma'_f}$. By Lemma 3.3(i),

$$\psi: (\bar{P}_f)_{\bar{\gamma}_f} \to \tilde{P}_{\tilde{\gamma}}$$

is an $S\tau_f$-isomorphism, while by Lemma 3.3(ii),

$$(\bar{P}_{\bar{\gamma}})_f \to (\bar{P}_f)_{\bar{\gamma}f}, \; x \mapsto x$$

(whose underlying map is the identity map on $\bar{P}_f$) is a f_τ-homomorphism. Hence:

(C) $\psi: (\bar{P}_{\bar{\gamma}})_f \to \tilde{P}_{\tilde{\gamma}}$ *is a bijective f_τ-homomorphism.*

(B) and (C) (together with the fact f_τ is epic) imply (A).

(Ad (iii). We must show that

$$(\psi_* \bar{q}_{(f)})(\tilde{p} \times_{S\tau_f} \tilde{p}') = q_{(f)}(\tilde{p})\, q'_{(f)}(\tilde{p}') \tag{3}$$

for all $\tilde{p}$ in P_f and $\tilde{p}'$ in P'_f. Let

$$\tilde{p} = \sum_{i=1}^{m} p_i \otimes_R s_i\,, \qquad \tilde{p}' = \sum_{j=1}^{n} p'_j \otimes_R s'_j$$

(with all p_i in P, all p'_j in P', all s_i and s'_j in S).

In the following computation, which verifies (3), the symbol $\ll$ is used to denote the usual lexicographic ordering on ordered pairs of integers, i.e.,

$$(m, n) \ll (m_1, n_1) \Leftrightarrow [(m < m_1) \text{ or } (m = m_1 \text{ and } n < n_1)].$$

$$q_{(f)}(\tilde{p}) = \sum_i q(p_i)\, {s_i}^2 + \sum_{i<J} B_q(p_i, p_I)\, s_i s_I\,,$$

$$q'_{(f)}(\tilde{p}') = \sum_j q'(p'_j)\, {s'_j}^2 + \sum_{j<J} B_{q'}(p'_j, p'_j)\, s'_j s'_j\,,$$

and

$$\begin{aligned}(\psi_* \bar{q}_{(f)})(\tilde{p} \otimes_{S\tau_f} \tilde{p}') &= \bar{q}_{(f)}(\psi^{-1}(\tilde{p} \otimes_{S\tau} \tilde{p}')) \\ &= \bar{q}_{(f)}\left(\sum_i \sum_j (p_i \otimes_{R\tau} p'_j) \otimes_R s_i s'_j\right) \\ &= \sum_i \sum_j \bar{q}(p_i \otimes_{R\tau} p'_j)\, {s_i}^2 {s'_j}^2 \\ &\quad + \sum_{(i,j) \ll (I,J)} B_{\bar{q}}(p_i \otimes_{R\tau} p'_j, p_I \otimes_{R\tau} p'_J)\, s_i s_I s'_j s'_J\,,\end{aligned}$$

whence, using Eqs. (1) through (1c) of the present section (which hold since by hypothesis $\tilde{\gamma}$ is a semi-composite of γ and γ'), and noting the identity

$$\begin{aligned}\sum_{(i,j) \ll (I,J)} F(i, j, I, J) &= \sum_i \sum_{j<J} F(i, j, i, J) + \sum_{i<I} \sum_j F(i, j, I, j) \\ &\quad + \sum_{i<I} \sum_{j<J} (F(i, j, I, J) + F(i, J, I, j)).\end{aligned}$$

we obtain

$$\begin{aligned}(\psi_*\bar{q}_{(f)})(\tilde{p} \otimes_{S\tau_f} \tilde{p}') &= \sum_i \sum_j q(p_i)\, q'(p_j')\, s_i^2 s_j'^2 \\ &\quad + \sum_i \sum_{j<J} q(p_i)\, B_{q'}(p_j', p_J')\, s_i^2 s_j' s_J' \\ &\quad + \sum_{i<I} \sum_j B_q(p_i, p_I)\, q'(p_j')\, s_i s_I s_j'^2 \\ &\quad + \sum_{i<I} \sum_{j<J} B_q(p_i, p_I)\, B_{q'}(p_j', p_J')\, s_i s_I s_j' s_J' \\ &= q_{(f)}(\tilde{p})\, q'_{(f)}(\tilde{p}')\end{aligned}$$

which completes the proof of Theorem 4.1.

We next wish to establish the connection between Definition 4.1 and the Gaussian composition of Definition 2.4 (cf. Theorems 4.5 and 4.6 below); for this purpose we first require the three following lemmas.

LEMMA 4.2. *Let $\tau = (\delta, b + 2R)$ be a form-type over R, so that (with the notation of Section 3) $R\tau = R[\sigma_b]$. Let E and F be $R\tau$-modules.*

Then there is an R-isomorphism

$$E \otimes_{R\tau} F \approx (E \otimes_R F)/K, \qquad e \otimes_{R\tau} f \mapsto (e \otimes_R f) + K,$$

where K is the submodule of $E \otimes_R F$ generated over R by the set of all

$$(\sigma_b e) \otimes_R f - e \otimes_R (\sigma_b f) \qquad (e \text{ in } E, f \text{ in } F).$$

Proof. We may give the R-module $(E \otimes_R F)/K$ the sturcture of an $R\tau$-module by setting

$$\sigma_b((e \otimes_R f) + K) = [(\sigma_b e) \otimes_R f] + K = [e \otimes_R (\sigma_b f)] + K.$$

It is then readily verified that the $R\tau$-bilinear map

$$E \times F \to (E \otimes_R F)/K, \qquad (e, f) \to (e \otimes_R f) + K$$

has the universal property which characterizes a tensor product of E and F over $R\tau$.

LEMMA 4.3. *Let the R-modules F and F' be free over R on*

$$B = \{f_1, \ldots, f_m\} \qquad \text{and} \qquad B' = \{f_1', \ldots, f_n'\},$$

respectively, and let the R-homomorphism $\phi: F \to F'$ *be represented with respect to these free bases by the* $n \times m$ *matrix* $T = (t_{ij})$ *over* R [*so that*

$$\phi\left(\sum r_i f_i\right) = \sum s_j f'_j \qquad (\text{all } r_i \text{ and } s_j \text{ in } R)$$

holds if and only if $T^t(r_1, \ldots, r_m) = {}^t(s_1, \ldots, s_n)$].

Then ϕ *is onto, if and only if,* $n \leqslant m$ *and the* $n \times n$ *subdeterminants of* T *generate the unit ideal in* R. *Moreover, if this is the case, and if* $D(i_1, \ldots, i_n)$ *denotes the* $n \times n$ *subdeterminant of* T *whose* jth *column is the* i_jth *column of* T, *then* $\operatorname{Ker} \phi$ *is generated over* R *by the elements*

$$\lambda(i_0, \ldots, i_n) = \sum_{s=0}^{n} (-1)^s D(i_0, \ldots, \hat{i}_s, \ldots, i_n) f_{i_s}, \tag{4}$$

where $i_0, \ldots, i_n$ *range from* 1 *to* m *and the caret over* i_s *indicates it is to be deleted.*

Remark. This lemma and the following Lemma 4.4 do not require the hypothesis that 2 is not a zero-divisor on R.

Proof of Lemma 4.3. Suppose first ϕ is onto, so there exist

$$e_i = \sum_{j=1}^{m} u_{ij} f_j \qquad (1 \leqslant i \leqslant n, \text{ all } u_{ij} \text{ in } R)$$

in F such that $\phi(e_i) = f'_i$. Setting $U = (u_{ij})$, it follows that $T^t U$ is the $n \times n$ identity matrix, so $\det(T^t U) = 1$. It is known that $\det(T^t U)$ is 0 if $n \geqslant m$, and otherwise is the sum of the products of the corresponding $n \times n$ subdeterminants of the $n \times m$ matrices T and U. Hence, $n \leqslant m$ and the $n \times n$ subdeterminants of T generate the unit ideal in R.

Suppose next that $n \leqslant m$ and that there exist

$$E(i_1, \ldots, i_n) \qquad (1 \leqslant i_1 < \cdots < i_n \leqslant m)$$

in R such that

$$\sum_{1 \leqslant i_1 < \cdots < i_n \leqslant m} D(i_1, \ldots, i_n)\, E(i_1, \ldots, i_n) = 1. \tag{5}$$

It must be shown that then ϕ is onto and $\operatorname{Ker} \phi$ is generated over R by the elements of the form (4).

We first show that f'_1 is in $\operatorname{Im} \phi$, i.e., that there exist $u_1, \ldots, u_m$ in R such that

$$\sum_{j=1}^{m} t_{ij} u_j = (1 \text{ if } i = 1,\ 0 \text{ if } 2 \leqslant i \leqslant n). \tag{6}$$

If $D(1, 2,..., n)$ is a unit in R, we may set $u_{n+1} = \cdots = u_{m=0}$ and solve (6) as a system of n equations in the n remaining unknowns $u_1, ..., u_n$, obtaining by Cramer's rule

$$u_j = \Delta_{1j}(1, 2,..., n)/D(1, 2,..., n) \qquad (1 \leqslant j \leqslant n),$$

where $\Delta_{1j}(1, 2,..., n)$ is the cofactor of t_{1j} in $D(1, 2,..., n)$. Whether or not $D(1, 2,..., n)$ is a unit in R,

$$\sum_{j=1}^{n} t_{ij}\Delta_{1j}(1, 2,..., n) = (D(1, 2,..., n) \text{ if } i = 1, 0 \text{ if } 2 \leqslant i \leqslant n),$$

i.e.,

$$\phi\left(\sum_{j=1}^{n} \Delta_{1j}(1, 2,..., n)f_j\right) = D(1, 2,..., n)f'_1.$$

Similarly, all $D(i_1, ..., i_n)f'_1$ lie in $\operatorname{Im}\phi$, so by (5), f'_1 is in $\operatorname{Im}\phi$. The same argument shows that $f'_2, ..., f'_n$ lie in $\operatorname{Im}\phi$, so ϕ is onto. [In more detail: let

$$\Delta_{ij}(j_1, ..., j_n)$$

denote the cofactor, in the determinant $D(j_1, ..., j_n)$, of t_{ij} if j is one of $j_1, ..., j_n$, and denote 0 otherwise; then

$$\phi\left(\sum_{j=1}^{m} \Delta_{ij}(j_1, ..., j_n)f_j\right) = D(j_1, ..., j_n)f'_i$$

so, by (5),

$$\sum_{j=1}^{m} \sum_{1 \leqslant j_1 < \cdots < j_n \leqslant m} \Delta_{ij}(j_1, ..., j_n)\, E(j_1, ..., j_n)f_j$$

is mapped by ϕ into f'_i.]

Finally, we must show that

$$\operatorname{Ker}\phi = K(B, B', \phi), \tag{7}$$

where $K(B, B', \phi)$ is the submodule of F generated over R by the set of all elements

$$\lambda(i_0, ..., i_n) \qquad (1 \leqslant i_0, ..., i_n \leqslant m)$$

in (4), or equivalently (since λ is alternating in the indices $1_0, ..., i_n$) by the set of all elements

$$\lambda(i_0, ..., i_n) \qquad (i \leqslant i_0 < \cdots < i_n \leqslant m).$$

We assume in proving (7) *that R is a quasi-local ring.* (This reduction is justified by a standard localization argument: For every maximal ideal M of R, let

$$B_M = \{(f_1)_M, ..., (f_m)_M\}, \qquad B'_M = \{(f'_1)_M, ..., (f'_m)_M\};$$

then F_M and F'_M are free over R_M on B_M and B'_M, respectively, and

$$\mathrm{Ker}(\phi_M) = (\mathrm{Ker}\,\phi)_M\,, \qquad K(B_M\,, B'_M\,, \phi_M) = (K(B,\, B',\, \phi))_M\,,$$

and, therefore, to prove (7), it suffices to prove

$$\mathrm{Ker}(\phi_M) = K(B_M\,, B'_M\,, \phi_M)$$

for every maximal ideal M of R.)

We next verify that $K(B,\, B',\, \phi)$ is independent of the choice of free basis B for F. Let us choose a new free basis $\bar{B} = \{\bar{f}_1\,, \ldots, \bar{f}_m\}$ for F over R, and compute the effect of this change of basis on the elements in (4). Let

$$\bar{f}_i = \sum_{j=1}^{m} u_{ji} f_j \qquad (1 \leqslant i \leqslant m, \text{ all } u_{ji} \text{ in } R);$$

then $U = (u_{ij})$ is a $m \times m$ matrix over R whose determinant is a unit in R. For $1 \leqslant s \leqslant m$, let $u(i_1\,, \ldots, i_s \mid j_1\,, \ldots, j_s)$ denote the $s \times s$ subdeterminant of U formed from rows $i_1\,, \ldots, i_s$ and columns $j_1\,, \ldots, j_s$. Then ϕ is represented with respect to the free bases $\bar{B}$ and B' by the $n \times n$ matrix $\bar{T} = TU$. The $n \times n$ subdeterminants $\bar{D}(i_1\,, \ldots, i_n)$ of $\bar{T}$ are given by the formula

$$\bar{D}(i_1\,, \ldots, i_n) = \sum_{1 \leqslant j_1 < \cdots < j_n \leqslant m} u(j_1\,, \ldots, j_n \mid i_1\,, \ldots, i_n)\, D(j_1\,, \ldots, j_n). \tag{8}$$

The effect of these replacements on (4) is given by

$$\begin{aligned}
\bar{\lambda}(i_0\,, \ldots, i_n) &= \sum_{s=0}^{n} (-1)^s\, \bar{D}(i_0\,, \ldots, \hat{i}_s\,, \ldots, i_n)\, \bar{f}_{i_s} \\
&= \sum_{s=0}^{n} \sum_{j_1 < \cdots < j_n} \sum_{j} (-1)^s\, u(j_1\,, \ldots, j_n \mid i_0\,, \ldots, \hat{i}_s\,, \ldots, i_n) u_{j, i_s}\, D(j_1\,, \ldots, j_n) f_j \\
&= \sum_{j_1 < \cdots < j_n} u(j, j_1\,, \ldots, j_n \mid i_0\,, \ldots, i_n)\, D(j_1\,, \ldots, j_n) f_j \\
&= \sum_{j} \sum_{s=0}^{n} \sum_{j_1 < \cdots < j_s < j < j_{s+1} < \cdots < j_n} u(j, j_1\,, \ldots, j_n \mid i_0\,, \ldots, i_n)\, D(j_1\,, \ldots, j_n) f_j \\
&= \sum_{s=0}^{n} \sum_{k_0 < \cdots < k_n} (-1)^s\, u(k_0\,, \ldots, k_n \mid i_0\,, \ldots, i_n)\, D(k_0\,, \ldots, \hat{k}_s\,, \ldots, k_n) f_{k_s} \\
&\quad \sum_{k_0 < \cdots < k_n} u(k_0\,, \ldots, k_n \mid i_0\,, \ldots, i_n(\, \lambda(k_0\,, \ldots, k_n).
\end{aligned} \tag{9}$$

Thus, the submodule $K(\bar{B}, B', \phi)$ generated by these $\bar{\lambda}$ is contained in $K(B, B', \phi)$ and (by a symmetry argument) equals $K(B, B', \phi)$.

It thus suffices to verify (7) for the following special choice of free basis B for F (for given B' and ϕ): pick f_i $(1 \leqslant i \leqslant n)$ in F such that $\phi(f_i) = f_i'$; then F is the direct sum of $Rf_1 \oplus \cdots \oplus Rf_n$ and $\operatorname{Ker}\phi$, and since we are assuming R is quasi-local, there thus exists a free basis $\{f_{n+1}, \ldots, f_m\}$ for $\operatorname{Ker}\phi$ over R; let $B = \{f_1, \ldots, f_m\}$. ϕ is represented by the $n \times n$ matrix $T = (I_n \mid 0)$ with respect to these free bases B and B'. The only nonzero $n \times n$ subdeterminant of T is $D(1, 2, \ldots, n) = 1$, and so the only nonzero $\lambda(i_0, \ldots, i_n)$ with $i_0 < \cdots < i_n$ are given by

$$\lambda(1, 2, \ldots, n, i) = (-1)^n f_i \qquad (n < i \leqslant m).$$

Thus, $K(B, B', \phi)$ is generated over R by $f_{n+1}, \ldots, f_m$ and so coincides with $\operatorname{Ker}\phi$, which completes the proof of the lemma.

Lemma 4.3 has the following converse.

LEMMA 4.4. *Let F and F' be modules free over the ring R on*

$$B = \{f_1, \ldots, f_m\} \qquad \text{and} \qquad B' = \{f_1', \ldots, f_n'\},$$

respectively, and let $\phi: F \to F'$ be a surjective R-homomorphism represented with respect to these free bases by the $n \times m$ matrix $T = (t_{ij})$ over R. Let $D(i_1, \ldots, i_n)$ denote the $n \times n$ subdeterminant of T whose jth column is the i_jth column of T. Finally, let

$$d(i_1, \ldots, i_n) \qquad (1 \leqslant i_1 < \cdots < i_n \leqslant m)$$

be elements of R with the property that $\operatorname{Ker}\phi$ is generated over R by the elements

$$l(i_0, \ldots, i_n) = \sum_{s=0}^{n} (-1)^s d(i_0, \ldots, \hat{i}_s, \ldots, i_n) f_{i_s} \qquad (1 \leqslant i_0 < \cdots < i_n \leqslant m).$$

Then it follows that there exists a unit u in R such that

$$d(i_1, \ldots, i_n) = uD(i_1, \ldots, i_n) \qquad (1 \leqslant i_1 < \cdots < i_n \leqslant m). \tag{10}$$

Proof. Since ϕ is an epimorphism, the $D(i_1, \ldots, i_n)$ generate the unit ideal over R by Lemma 4.3. It follows that to show the existence of a unit u in R satisfying (10). it suffices to show there exist elements u and v in R satisfying the *linear* equations

$$d(i_1, \ldots, i_n) = uD(i_1, \ldots, i_n),\ D(i_1, \ldots, i_n) = vd(i_1, \ldots, i_n) \tag{10a}$$

for $1 \leqslant i_1 < \cdots < i_n \leqslant m$, since then

$$(uv - 1)\, D(i_1, \ldots, i_n) = 0 \qquad (1 \leqslant i_1 < \cdots < i_n \leqslant m)$$

whence $uv = 1$ and u is a unit. This observation enables us to apply the method of localization; thus, in the remainder of the proof, it will be assumed that R is a quasi-local ring.

Since R is quasi-local and $\operatorname{Im}\phi$ is free, $\operatorname{Ker}\phi$ is a direct summand of F and there exists a free basis

$$\bar{B} = \{\bar{f}_1, \ldots, \bar{f}_n\}$$

for F over R such that

$$\begin{aligned} \phi(\bar{f}_i) &= f_i' \qquad (1 \leqslant i \leqslant n) \\ &= 0 \qquad (n < i \leqslant m) \end{aligned}$$

which implies that $\operatorname{Ker}\phi$ is free over R on $\{\bar{f}_{n+1}, \ldots, \bar{f}_m\}$. Thus, ϕ is represented with respect to the free bases $\bar{B}$ and B' by the $n \times m$ matrix

$$T = (I_n \mid 0)$$

whose $m \times m$ subdeterminants are given by

$$\begin{aligned} \bar{D}(i_1, \ldots, i_n) &= 1 \qquad \text{if} \quad i_1 = 1, \ldots, i_n = n \\ &= 0 \qquad \text{otherwise if} \quad 1 \leqslant i_1 < \cdots < i_n \leqslant m. \end{aligned}$$

We have

$$\bar{f}_i = \sum_{j=1}^{m} u_{ji} f_j \,, \; f_i = \sum_{j=1}^{m} v_{ji} \bar{f}_j \qquad (1 \leqslant i \leqslant m, \text{ all } u_{ji} \text{ and } v_{ji} \text{ in } R)$$

so that $U = (u_{ij})$, $V = (v_{ij})$ are inverse $m \times m$ matrices over R, and

$$\bar{T} = TU, \qquad T = \bar{T}V.$$

For $1 \leqslant s \leqslant m$, let $u(i_1, \ldots, i_s \mid j_1, \ldots, j_s)$ denote the $s \times s$ subdeterminant of U formed by rows $i_1, \ldots, i_s$ and columns $j_1, \ldots, j_s$, let $v(i_1, \ldots, i_s \mid j_1, \ldots, j_s)$ be formed similarly from V, and let

$$\Delta(s) = \{(i_1, \ldots, i_s) \colon 1 \leqslant i_1 < \cdots < i_s \leqslant m\}.$$

We have, for I and J in $\Delta(s)$,

$$\begin{aligned} \sum_{K \in \Delta(s)} u(I \mid K)\, v(K \mid J) &= 1 \qquad \text{if } I = J \\ &= 0 \qquad \text{otherwise} \\ \sum_{K \in \Delta(s)} v(I \mid K)\, u(K \mid J) &= 1 \qquad \text{if } I = J \\ &= 0 \qquad \text{otherwise} \end{aligned} \tag{11}$$

(cf. [30]; classically, this result was expressed by saying: The sth compounds of the inverse matrices U and V are again inverse). Also, if I is in $\Delta(n)$

$$\begin{aligned} \bar{D}(I) &= \sum_{J\in\Delta(n)} u(J \mid I)\, D(J), \\ D(I) &= \sum_{J\in\Delta(n)} v(J, I)\, \bar{D}(J) = v(1, 2,..., n \mid I) \end{aligned} \tag{12}$$

(cf. formula (8) in the proof of Lemma 4.3). Let us, accordingly, define $\bar{d}(I)$, for I in $\Delta(n)$, by

$$\bar{d}(I) = \sum_{J\in\Delta(n)} u(J \mid I)\, d(J)$$

from which it follows, using (11), that

$$d(I) = \sum_{J\in\Delta(n)} v(J \mid I)\, \bar{d}(J) \qquad (I \in \Delta(n)). \tag{13}$$

If we now set

$$l(i_0,..., i_n) = \sum_{s=0}^{n} (-1)^s\, d(i_0,..., i_s,..., i_n) f_{i_s} \qquad (1 \leqslant i_0 < \cdots < i_n \leqslant m),$$

then, replacing every λ and D by l and d, respectively, in (9) of Lemma 4.3, we see that

$$\bar{l}(I) = \sum_{J\in\Delta(n+1)} u(J \mid I)\, l(J),$$

whence (by (11))

$$l(I) = \sum_{J\in\Delta(n+1)} v(J \mid I)\, \bar{l}(J),$$

from which it follows that the $\bar{l}(I)$ $(I \in \Delta(n+1))$ generate the same module over R that the $l(I)$ do; by hypothesis, this is

$$\operatorname{Ker} \phi = Rf_{n+1} + \cdots + Rf_m .$$

This implies that

$$\bar{d}(I) = 0 \qquad \text{if} \quad I \neq (1, 2,..., n)\ (I \in \Delta(n)) \tag{14}$$

for if $(i_1,..., i_n) \neq (1,..., n)$, we may find

$$1 \leqslant j_0 < \cdots < j_n \leqslant m, \qquad 0 \leqslant s \leqslant m,$$

such that

$$j_s \leqslant n, \qquad (j_0, \ldots, \hat{j}_s, \ldots, j_n) = (l_1, \ldots, i_n)$$

and then $\bar{d}(i_1, \ldots, i_n)$, being the coefficient of $\bar{f}_{j_s}$ in $\bar{l}(j_0, \ldots, j_n)$ which lies in $Rf_{n+1} \oplus \cdots \oplus Rf_m$, must equal 0. Hence, all $\bar{l}(I)$ are 0 ($i \in \Delta(n+1)$) except for

$$\bar{l}(1, \ldots, n, i) = (-1)^n \bar{d}(1, \ldots, n) f_i \qquad (n < i \leqslant m)$$

and since these generate $R\bar{f}_{n+1} \oplus \cdots \oplus R\bar{f}_m$, it follows that $\bar{d}(1, \ldots, n)$ is a unit in R. Using (12), (13), and (14), we obtain, for all I in $\Delta(n)$,

$$d(I) = v(1, \ldots, n \mid I)\, \bar{d}(1, \ldots, n) = D(I)\, \bar{d}(1, \ldots, n)$$

which (with $u = \bar{d}(1, \ldots, n)$) is (10).

THEOREM 4.5. *Let the numerical binary quadratic form*

$$[A, B, C]^L$$

over R be a Gaussian composite over R (cf. Definition 2.4) of the numerical forms

$$[a, b, c]^L \qquad \text{and} \qquad [a', b', c']^L$$

over R. Let γ and γ' be free oriented forms over R, associated with the numerical forms $[a, b, c]^L$ and $[a', b', c']^L$ respectively (cf. Definition 1.11). Then γ and γ' have a semi-composite, which is a free form associated with $[A, B, C]^L$.

Proof. Let

$$\gamma = (P, \epsilon, q), \qquad \gamma' = (P', \epsilon', q')$$

be represented, respectively, by $[a, b, c]^L$ and $[a', b', c']^L$ with respect to the properly oriented free bases $\{e_1, e_2\}$ and $\{e_1', e_2'\}$, respectively, so that

$$e_1 \wedge e_2 = \epsilon, \qquad e_1' \wedge e_2' = \epsilon',$$

$$q(x_1 e_1 + x_2 e_2) = a x_1^2 + b x_1 x_2 + c x_2^2,$$

$$q'(x_1 e_1' + x_2 e_2') = a' x_1^2 + b' x_1 x_2 + c' x_2^2$$

(all x_1 and x_2 in R). By hypothesis, there exists a 2×4 matrix

$$\Sigma = \begin{pmatrix} m_0, & m_1, & m_2, & m_3 \\ n_0, & n_1, & n_2, & n_3 \end{pmatrix}$$

over R, whose six 2×2 subdeterminants

$$d_{ij} = m_i n_j - m_j n_i \qquad (0 \leqslant i < j \leqslant 3) \tag{15}$$

generate the unit ideal in R, and such that (cf. Definition 2.4)

$$[a, b, c]^L = q_\Sigma = [d_{01}, d_{03} - d_{12}, d_{23}]^L, \tag{16}$$

$$[a', b', c']^L = q'_\Sigma = d_{02}, d_{03} + d_{12}, d_{13}]^L, \tag{17}$$

$$[A, B, C]^L = Q_\Sigma = [n_1n_2 - n_0n_3, m_0n_3 + m_3n_0 - m_1n_2 - m_2n_1, m_1m_2 - m_0m_3]^L \tag{18}$$

By Proposition 2.4, $q_\Sigma = [a, b, c]^L$ and $q'_\Sigma = [a', b', c']^L$ have the same discriminant δ and parity π; hence γ and γ' are both forms of type $\tau = (\delta, \pi)$. Note that

$$\pi = b + 2R = b' + 2R.$$

$P \otimes_R P'$ is free over R on the four elements

$$e_{ij} = e_i \otimes_R e'_j \qquad (i, j = 1 \text{ or } 2)$$

and by Lemma 4.2, the R_τ-module

$$\bar{P} = P_\gamma \otimes_{R_\tau} P'_{\gamma'}$$

is the image of the R-homomorphism

$$\phi_1 : P \otimes_R P' \to P_\gamma \otimes_{R_\tau} P'_{\gamma'}, \; p \otimes_R p' \to p \otimes_{R_\tau} p'$$

whose kernel is generated over R by the four elements

$$k_{ij} = (\sigma e_i) \otimes_R e'_j - e_i \otimes_R (\sigma_b e'_j) \qquad (i, j = 1 \text{ or } 2).$$

By Proposition 3.2, Corollary 1, we have

$$\sigma_b e_1 = -be_1 + ae_2, \qquad \sigma_b e_2 = -ce_1,$$

$$\sigma_b e'_1 = -\tfrac{1}{2}(b' + b)e_1 + a'e'_2, \qquad \sigma_b e'_2 = -c'e'_1 + \tfrac{1}{2}(b' - b)e'_2$$

whence

$$\begin{aligned}
k_{11} &= \tfrac{1}{2}(b' - b)e_{11} - a'e_{12} + ae_{21} && (= d_{12}e_{11} - d_{02}e_{12} + d_{01}e_{21}),\\
k_{12} &= c'e_{11} - \tfrac{1}{2}(b' + b)e_{12} + ae_{22} && (= d_{13}e_{11} - d_{03}e_{12} + d_{01}e_{22}),\\
k_{21} &= -ce_{11} + \tfrac{1}{2}(b' + b)e_{21} - a'e_{22} && (= -d_{23}e_{11} + d_{03}e_{21} - d_{02}e_{22}),\\
k_{22} &= -ce_{12} + c'e_{21} - \tfrac{1}{2}(b' - b)e_{22} && (= -d_{23}e_{12} + d_{13}e_{21} - d_{12}e_{22}).
\end{aligned} \tag{19}$$

It follows from Lemma 4.3 (with $m = 4$, $n = 2$, $F = P \otimes_R P'$, $F' = R^2$, $(f_1, f_2, f_3, f_4) = (e_{11}, e_{12}, e_{21}, e_{22})$, and $T = \Sigma$) that the R-homomorphism $\phi_2 : P \otimes_R P' \to R^2$ defined by

$$\phi_2(x_0e_{11} + x_1e_{12} + x_2e_{21} + x_3e_{22}) = {}^t\left(\sum m_ix_i, \sum n_ix_i\right) \qquad (x_i \text{ in } R)$$

is surjective (since by hypothesis the 2×2 subdeterminants of Σ generate the unit ideal in R) and has its kernel generated over R by exactly the four k_{ij} listed above. Since ϕ_1 and ϕ_2 are both epic and have the same kernel, we conclude that there exists an R-isomorphism

$$\phi\colon \bar{P} = P_\gamma \otimes_R P'_{\gamma'} \to R^2,\ \phi_1(u) \mapsto \phi_2(u)$$

which maps

$$x_0e_1 \otimes_{R_T} e'_1 + x_1e_1 \otimes_{R_T} e'_2 + \otimes_2 e_2 \times_{R_T} e'_1 + \otimes_3 e_2 \times_{R_T} e'_2$$

(where the x_i lie in R) into

$${}^t\left(\sum m_ix_i, \sum n_ix_i\right).$$

Thus, $\bar{P}$ is free over R on the elements E_1, E_2 mapped by ϕ into $\binom{1}{0}$, $\binom{0}{1}$, respectively. Note that

$$\begin{aligned} e_1 \otimes_{R_T} e'_1 &= m_0E_1 + n_0E_2, & e_1 \otimes_{R_T} e'_2 &= m_1E_1 + n_1E_2, \\ e_2 \otimes_{R_T} e'_1 &= m_2E_1 + n_2E_2, & e_2 \otimes_{R_T} e'_2 &= m_3E_1 + n_3E_2 \end{aligned} \tag{20}$$

the first of these equations, for instance, following from

$$\phi(e_1 \otimes_{R_T} e'_1) = {}^t(m_0, n_0) = \phi(m_0E_1 + n_0E_2)$$

and the fact that ϕ is an isomorphism.

Let $\bar{\epsilon}$ be the rank 2 R-orientation $E_1 \wedge E_2$ on $\bar{P}$, let $\bar{q}$ be the L-quadratic form

$$\bar{q}\colon \bar{P} \to R,\ x_1E_1 + x_2E_2 \mapsto Ax_1^2 + Bx_1x_2 + Cx_2^2$$

on $\bar{P}$ over R, and let

$$\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q}).$$

We are done if we show $\bar{\gamma}$ satisfies conditions (i), (ii), and (iii) of Definition 4.1, since $\bar{\gamma}$ is a free form which by construction is associated with $[A, B, C^L]$.

$\bar{\gamma}$ satisfies (i). By Proposition 2.4 $[A, B, C]^L$, $[a, b, c]^L$, and $[a', b', c']^L$ are of the same form-type over R; hence, by Proposition 1.16, so are $\bar{\gamma}$, γ and γ'.

$\bar{\gamma}$ *satisfies* (ii). With the notation of Definition 3.3, it suffices to show that

$$T_b(\bar{\gamma})[e_i \otimes_{R\tau} e'_j] = [T_b(\gamma)e_i] \otimes_{R\tau} e'_j \qquad (i, j = 1 \text{ or } 2) \tag{21}$$

since the left-hand side of (21) represents the product of σ_b with $e_i \otimes_{R\tau} e'_j$ in the $R\tau$-module structure $\bar{P}_{\bar{\gamma}}$ on $\bar{P}$, while the right-hand side denotes the same product in the $R\tau$-module structure $P_\gamma \otimes_{R\tau} P'_{\gamma'}$ [and since $R\tau = R[\sigma_b]$ and the $e_i \otimes_{R\tau} e'_j$ generate $\bar{P}$ over R].

Using Proposition 3.2, Corollary 1, and (19), we obtain

$$\begin{aligned} T_b(\bar{\gamma})[e_1 \otimes_{R\tau} e'_1] &= T_b(\bar{\gamma})[m_0E_1 + n_0E_2] \\ &= -[\tfrac{1}{2}(B + b)m_0 + Cn_0]E_1 + [Am_0 + \tfrac{1}{2}(B - b)n_0]E_2 , \end{aligned} \tag{22}$$

$$T_b(\gamma)e_1 = -be_1 + ae_2 ,$$

$$\begin{aligned} [T_b(\gamma)e_1] \otimes_{R\tau} e'_1 &= -be_1 \otimes e'_1 + ae_2 \otimes e'_1 \\ &= -b(m_0E_1 + n_0E_2) + a(m_2E_1 + n_2E_2), \end{aligned} \tag{23}$$

and to verify that (22) and (23) are equal, i.e., that

$$-\tfrac{1}{2}(B + b)m_0 - Cn_0 = -bm_0 + am_2 , \tag{24}$$

and

$$Am_0 + \tfrac{1}{2}(B - b)n_0 = -bn_0 + an_2 \tag{25}$$

we need only substitute from (15), (16), and (18), obtaining

$$-m_0{}^2n_3 + m_0m_1n_2 - m_1m_2n_0 + m_0m_3n_0$$

as the common value for both sides of (24), and

$$m_3n_0{}^2 - m_2n_0n_1 + m_0n_1n_2 - m_0n_0n_3$$

as the common value for both sides of (25). This proves (21) when $(i, j) = (1, 1)$; the computations in the three remaining cases $(i, j) = (1, 2)$, $(2, 1)$ or $(2, 2)$ are similar, and are here omitted.

$\bar{\gamma}$ *satisfies* (iii). Let $p \in P$, $p' \in P'$; then

$$p = x_1e_1 + x_2e_2 , \qquad p' = x'_1e'_1 + x'_2e'_2$$

with x_i and x'_1 in R. By (20), $p \otimes_{R\tau} p' = X_1E_1 + X_2E_2$, with

$$X_1 = m_0x_1x'_1 + m_1x_1x'_2 + m_2x_2x'_1 + m_3x_2x'_2 ,$$

$$X_2 = n_0x_1x'_1 + n_1x_1x'_2 + n_2x_2x'_1 + n_3x_2x'_2 ,$$

whence, by Proposition 2.4,

$$\bar{q}(p \otimes_{R\tau} p') = Q_\Sigma \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = q_\Sigma \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} q'_\Sigma \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} = q(p)\, q'(p').$$

This completes the proof of Theorem 4.5; for later use, we record in the form of a corollary some additional information also established in the course of the preceding proof:

COROLLARY. *Let*

$$\Sigma = \begin{pmatrix} m_0 , & m_1 , & m_2 , & m_3 \\ n_0 , & n_1 , & n_2 , & n_3 \end{pmatrix}$$

be a unimodular 2×4 *matrix over* R, *and let*

$$\gamma = (P, e_1 \wedge e_2 , q), \qquad \gamma' = (P', e'_1 \wedge e'_2 , q')$$

where P, P' *are free over* R *on* $\{e_1 , e_2\}$, $\{e'_1 , e'_2\}$, *respectively, and*

$$q(x_1 e_1 + x_2 e_2) = q_\Sigma \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \; q'(x_1 e'_1 + x_2 e'_2) = q'_\Sigma \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$$

for all x_1 *and* x_2 *in* R. *Then* γ *and* γ' *have a semi-composite*

$$(P_\gamma \otimes_{R\tau} P'_{\gamma'} , E_1 \wedge E_2 , q)$$

constructed as follows: *There is an* R*-isomorphism* $\phi: P_\gamma \otimes_{R\tau} P'_{\gamma'} \approx R^2$, *well defined by*

$$\phi(x_0 e_1 \otimes_{R\tau} e'_1 + x_1 e_1 \otimes_{R\tau} e'_2 + x_2 e_2 \otimes_{R\tau} e'_1 + x_3 e_2 \, {}_R\!\otimes_\tau e'_2) = {}^t\left(\sum m_i x_i , \sum n_i x_i\right)$$

for all x_0 , x_1 , x_2 , x_3 *in* R; *we then define* $E_1 = \phi^{-1}\binom{1}{0}$, $E_2 = \phi^{-1}\binom{0}{1}$, *and* q *by*

$$q(x_1 E_1 + x_2 E_2) = Q_\Sigma \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad (\textit{all } x_1 , x_2 \textit{ in } R).$$

Moreover, Eqs. (20) *are valid in this situation.*

THEOREM 4.6. *Let* $\gamma = (P, \epsilon, q)$ *and* $\gamma' = (P', \epsilon', q')$ *be free oriented forms over* R, *of the same type* τ, *and associated with the numerical forms* $[a, b, c]^L$ *and* $[a', b', c']^L$ *over* R, *respectively. Then the following three statements are equivalent*:

(a) γ *and* γ' *have a semi-composite which is a free form over* R;

(b) $P_\gamma \otimes_R P'_{\gamma'}$ *is free over* R *of rank* 2;

(c) $[a, b, c]^L$ *and* $[a', b', c']^L$ *have a Gaussian composite over* R.

Proof. We shall prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).

(a) $\Rightarrow$ (b). This is immediate, using Definition 4.1 (ii).

(b) $\Rightarrow$ (c). Let γ (and γ') be represented by $[a, b, c]^L$ (and $[a', b', c']^L$, respectively) with respect to the properly oriented free bases $\{e_1, e_2\}$ (and $\{e_1', e_2'\}$, respectively). Let P denote $P_\gamma \otimes_{R_T} P_{\gamma'}'$, considered as an R-module, and let P be free over R on E_1 and E_2.

By Lemma 4.2, there is an R-epimorphism

$$\phi_1 : P \otimes_R P' \to P,\ p \otimes_R p' \mapsto p \otimes_{R_T} p'$$

with Ker ϕ_1 generated over R by the four elements

$$k_{ij} = (\sigma_b e_i) \otimes_R e_j - e_i \otimes_R (\sigma_b e_j) \qquad (i, j = 1 \text{ or } 2).$$

These were computed in the proof of Theorem 4.5, and are given by the first halves of Eqs. (19) (the portions of (29) involving d_{ij}'s must here be ignored).

Let ϕ_1 be represented with respect to the free bases $B = \{e_{11}, e_{12}, e_{21}, e_{22}\}$ and $b' = \{E_1, E_2\}$ for $P \otimes_R P'$ and P, respectively, over R by the matrix

$$T = \begin{pmatrix} p_1, & p_2, & p_3, & p_4 \\ q_1, & q_2, & q_3, & q_4 \end{pmatrix}.$$

Lemma 4.4 is now applicable, with $m = 4$, $n = 2$, $\phi = \phi_1$, $e_{11} = f_1$, $e_{12} = f_2$, $e_{21} = f_3$, $e_{22} = f_4$

$$\begin{aligned} &d(1, 2) = a,\ d(1, 3) = a',\ d(1, 4) = \tfrac{1}{2}(b' + b),\ d(2, 3) = \tfrac{1}{2}(b' - b), \\ &d(2, 4) = c',\ d(3, 4) = c, \end{aligned} \tag{26}$$

because (by (19)) the $l(i_0, i_1, i_2)$ of that lemma then become

$$\begin{aligned} l(123) &= d(2, 3)f_1 - d(1, 3)f_2 + d(1, 2)f_3 \\ &= \tfrac{1}{2}(b' - b)e_{11} - a'e_{12} + ae_{21} = k_{11}, \\ l(124) &= c'e_{11} - \tfrac{1}{2}(b' + b)e_{12} + ac_{22} = k_{12}, \\ l(134) &= ce_{11} - \tfrac{1}{2}(b' + b)e_{21} + a'e_{22} = -k_{21}, \\ l(234) &= ce_{12} - c'e_{21} + \tfrac{1}{2}(b' - b)e_{22} = -k_{22}, \end{aligned}$$

and, hence, generate Ker ϕ_1 over R. Thus, there exists a unit u in R with

$$d(i, j) = u(p_i q_j - p_j q_i) \qquad (1 \leqslant i < j \leqslant 4). \tag{27}$$

Letting Σ denote the matrix

$$\begin{pmatrix} up_1, & up_2, & up_3, & up_4 \\ q_1, & q_2, & q_3, & q_4 \end{pmatrix}$$

it follows from (26), (27), and Definition 2.4 that

$$[a, b, c]^L = q_\Sigma\,, \qquad [a', b', c']^L = q'_\Sigma\,.$$

Since ϕ is surjective, the 2×2 subdeterminants of T generate the unit ideal over R, by Lemma 4.3, and hence, also Σ is unimodular. Thus, $[a, b, c]^L$ and $[a', b', c']^L$ have the Gaussian composite Q_Σ over R.

(c) $\Rightarrow$ (a). This is immediate, using Theorem 4.5.

COROLLARY. *If two forms γ and γ' over R possess a semi-composite over R, then they are comaximal, i.e.,*

$$\operatorname{div}\gamma + \operatorname{div}\gamma' = R.$$

Proof. Using Lemmas 1.11(ii) and 4.1 we reduce to the case where R is quasi-local, and so γ and γ' are free forms, associated, say, with the numerical forms

$$[a, b, c]^L \qquad \text{and} \qquad [a', b', c']^L$$

over R, respectively; these forms possess a Gaussian composite over R, by the preceding theorem, whence by Proposition 1.16 and 2.5,

$$R = Ra + Rb + Rc + Ra' + Rb' + Rc' = \operatorname{div}\gamma + \operatorname{div}\gamma'.$$

The following converse to Theorem 4.1 will be required for the proof of Theorems 4.8 and 4.9.

THEOREM 4.7. *Let $\gamma = (P, \epsilon, q)$ and $\gamma' = (P', \epsilon', q')$ be two forms of type τ over R. Let $\bar{P}$ denote the R-module underlying the $R\tau$-module $P_\gamma \otimes_R P'_{\gamma'}$, and, for every maximal ideal M of R, let*

$$\psi^M\colon \bar{P}_M \to (P_M)_{\gamma_M} \otimes_{R_M \tau_M} (P'_M)_{\gamma'_M}\,, \qquad (p \otimes p')_M \mapsto p_M \otimes p'_M$$

denote the R_M-isomorphism obtained from the canonical homomorphism $R \to R_M$ in accordance with Theorem 4.1.

Then a form $\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q})$ over R is a semi-composite of γ and γ', if and only if, for every maximal ideal M of R, $(\psi^M)_*\bar{\gamma}_M$ is a semi-composite of γ_M and γ'_M.

Proof. Only if: This is just a special case of Theorem 4.1.

If: Let

$$(\psi^M)_*\bar{\gamma}_M = \bar{\gamma}(M) = (\bar{P}(M), \bar{\epsilon}(M), \bar{q}(M)),$$

so ψ^M is a proper R_M-equivalence from $\bar{\gamma}_M$ to $\bar{\gamma}(M)$ (cf. Proposition 1.13) and $\bar{P}(M)$ is the R_M-module underlying

$$(P_M)_{\gamma_M} \otimes_{R_M \tau_M} (P'_M)_{\gamma'_M}\,.$$

Suppose that, for every maximal ideal M of R, $\bar{\gamma}(M)$ is a semi-composite of γ_M and γ'_M.

We shall prove that then $\bar{\gamma}$ is a semi-composite of γ and γ', by verifying conditions (i), (ii), and (iii) of Definition 4.1. (The reader will note that these verifications are essentially the same as the corresponding verifications in the proof of Theorem 4.1, except that (iii) is much simpler to verify in the present case; also, (ii) has been presented in different language.)

(Ad (i). Let $\bar{\tau}$ be the form-type of $\bar{\gamma}$. For every maximal ideal M of R, $\bar{\tau}_M$ is the form-type of $\bar{\gamma}_M$, and thus of the properly equivalent form $\bar{\gamma}(M)$. Since $\bar{\gamma}(M)$ is the semi-composite of γ_M and $(\gamma')_{M'}$ it has by (i) of Definition 4.1 the same form-type as these, namely, τ_M. Thus, $\bar{\tau}_M = \tau_M$ for every maximal ideal M of R, and so $\bar{\tau} = \tau$.

(Ad (ii). Let $\tau = (\delta, b + 2R)$, so, with the notation of Section 3, $R\tau = R[\sigma_b]$. By construction, $\bar{P}$ coincides with the R-module structure on $P_\gamma \otimes_{R\tau} (P')_{\gamma'}$. Thus, to show that $\bar{\gamma}$ satisfies condition (ii) of Definition 4.1 is equivalent to showing that multiplication by σ_b in the $R\tau$-module structure $\bar{P}_{\bar{\gamma}}$ on $\bar{P}$ coincides with multiplication by σ_b in the $R\tau$-module structure $P_\gamma \otimes_{R\tau} (P')_{\gamma'}$ on $\bar{P}$, i.e., to showing that (with the notation of Definition 3.3)

$$T_b(\bar{\gamma}) = T_b(\gamma) \otimes_{R\tau} \mathrm{Id}(P') \tag{28}$$

(where $\mathrm{Id}(P')$ denotes the identity map on P').

Let M be any maximal ideal of R. By Lemma 3.3(ii)

$$[T_b(\bar{\gamma})]_M = T_{b_M}(\bar{\gamma}_M)$$

so by Lemma 3.3(i) the following diagram commutes:

$$\begin{array}{ccc} \bar{P}_M & \xrightarrow{[T_b(\bar{\gamma})]_M} & \bar{P}_M \\ {\scriptstyle \psi^M}\downarrow & & \downarrow{\scriptstyle \psi^M} \\ \bar{P}(M) & \xrightarrow{T_{b_M}(\bar{\gamma}(M))} & \bar{P}(M) \end{array} \tag{29}$$

We may also verify that the following diagram commutes:

$$\begin{array}{ccc} \bar{P}_M & \xrightarrow{[T_b(\gamma) \otimes \mathrm{Id}]_M} & \bar{P}_M \\ {\scriptstyle \psi^M}\downarrow & & \downarrow{\scriptstyle \psi^M} \\ \bar{P}(M) & \xrightarrow{T_{b_M}(\gamma_M) \otimes \mathrm{Id}} & \bar{P}(M) \end{array} \tag{30}$$

by the following element-wise computation:

$$\psi^M([T_b(\gamma) \otimes \mathrm{Id}]_M (p \otimes_{R\tau} p')_M)$$
$$= \psi^M[(T_b(\gamma)\, p \otimes_{R\tau} p')_M] = (T_b(\gamma)p)_M \otimes_{R_M\tau_M} p'_M$$

which by Lemma 3.3 is

$$[T_{b_M}(\gamma_M)p_M] \otimes_{R_M\tau_M} p'_M = (T_{b_M}(\gamma_M) \otimes \mathrm{Id})(p_M \otimes_{R_M\tau_M} p'_M)$$
$$= (T_{b_M}(\gamma_M) \otimes \mathrm{Id})\, [\psi^M(p \otimes_{R\tau} p')_M].$$

By hypothesis, $\bar{\gamma}(M)$ is a semi-composite of γ_M and $(\gamma')_M$, these three forms being of type $\tau_M = (\delta_M, b_M + 2R_M)$, so

$$T_{b_M}(\bar{\gamma}(M)) = T_{b_M}(\gamma_M) \otimes \mathrm{Id}$$

and this, the fact that (29) and (30) commute, and the fact that ψ^M is an R_M-isomorphism, together imply that

$$[T_b(\bar{\gamma})]_M = [T_b(\gamma) \times \mathrm{Id}]_M . \tag{31}$$

The fact that (31) holds for every maximal ideal M of R implies (28).

(Ad (iii). We must show that, for all p in P and p' in P',

$$\bar{q}(p \times_{R\tau} p') = q(p)\, q'(p').$$

This follows from the fact that since, for every maximal ideal M of R,

$$(\psi^M)_*(\bar{P}_M, \bar{\epsilon}_{(M)}, \bar{q}_{(M)}) = (\bar{P}(M), \bar{\epsilon}(M), \bar{q}(M))$$

is a semi-composite of γ_M and $(\gamma')_M$, we thus have

$$[\bar{q}(p \otimes_{R\tau} p')]_M = \bar{q}_M((p \otimes_{R\tau} p')_M) = \bar{q}(M)(\psi^M(p \otimes_{R\tau} p'))$$
$$= \bar{q}(M)(p_M \otimes_{R_M\tau_M} (p')_M) = q_M(p_M)q'_M(p'_M) = [q(p)q'(p')]_M$$

holding for every maximal ideal M of R.

THEOREM 4.8. *Let the form $\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q})$ over R be a semi-composite of the forms γ and γ' over R. Then (cf. Definition* 1.12)

$$\mathrm{div}\, \bar{\gamma} = (\mathrm{div}\, \gamma)(\mathrm{div}\, \gamma').$$

Moreover, any other semi-composite of γ and γ' is then of the form $(\bar{P}, u\bar{\epsilon}, \bar{q})$, where u is a unit of R such that $1 - u$ annihilates $\mathrm{div}\, \bar{\gamma}$; *conversely, if u is such a unit of R, then $(\bar{P}, u\bar{\epsilon}, \bar{q})$ is a semi-composite of γ and γ'.*

Proof. Let M denote the set of all units u in R such that $1 - u$ annihilates $\operatorname{div} \bar{\gamma}$. Note that M forms a group under multiplication. Let

$$\gamma = (P, \epsilon, q), \qquad \gamma' = (P', \epsilon', q'),$$

and let τ denote the common form-type of γ and γ'. It follows from (ii) of Definition 4.1 that $\bar{P}$ is $P_\gamma \otimes_{R\tau} P'_{\gamma'}$ considered as an R-module, and that any other semi-composite of γ and γ' must also have $\bar{P}$ as underlying R-module.

We consider first the case in which R is quasi-local. Then P and P' are free over R, say, on $\{e_1, e_2\}$ and $\{e'_1, e'_2\}$, respectively, with

$$e_1 \wedge e_2 = \epsilon, \qquad e'_1 \wedge e'_2 = \epsilon'.$$

There exist a, b, c, a', b', c' in R such that

$$q(x_1e_1 + x_2e_2) = ax_1{}' + bx_1x_2 + cx_2{}^2, \; q'(x_1e'_1 + x_2e'_2) = a'x_1{}^2 + b'x_1x_2 + c'x_2{}^2$$

for all x_1 and x_2 in R. Similarly, $\bar{P}$ is free over R, so it follows from Theorem 4.6 that $[a, b, c]^L$ and $[a', b', c']^L$ have a Gaussian composite over R, i.e., that there exists a unimodular 2×4 matrix

$$\Sigma = \begin{pmatrix} m_0 , & m_1 , & m_2 , & m_3 \\ n_0 , & n_1 , & n_2 , & n_3 \end{pmatrix}$$

over R such that (cf. Definition 2.4)

$$[a, b, c]^L = q_\Sigma , \qquad [a', b', c']^L = q'_\Sigma .$$

Let

$$Q_\Sigma = [A, B, C]^L.$$

It follows from the corollary to Theorem 4.5 that there is an R-isomorphism ϕ: $\bar{P} \approx R^2$, which maps the element

$$x_0e_1 \otimes_{R\tau} e'_1 + x_1e_1 \otimes_{R\tau} e'_2 + x_2e_2 \otimes_{R\tau} e'_1 + x_3e_2 \otimes_{R\tau} e'_2$$

(with x_0 , x_1 , x_2 , x_3 in R) of $\bar{P} = P_\gamma \otimes_R P'_{\gamma'}$ into

$$^t\left(\sum m_ix_i , \sum n_ix_i\right),$$

and that if we set

$$E_1 = \phi^{-1}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; E_2 = \phi^{-1}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

(whence $\bar{P}$ is free over R on E_1 and E_2)

$$E_1 \wedge E_2 = \tilde{\epsilon}$$
$$\tilde{q}\colon \bar{P} \to R,\ x_1E_1 + x_2E_2 \mapsto Ax_1^2 + Bx_1x_2 + Cx_2^2 \qquad (x_1 \text{ and } x_2 \text{ in } R),$$
$$\tilde{\gamma} = (\tilde{P}, \tilde{\epsilon}, \tilde{q}),$$

then $\tilde{\gamma}$ is a semi-composite of γ and γ'.

Since $\bar{\gamma}$ and $\tilde{\gamma}$ are both semi-composites of γ and γ', it follows from (ii) of Definition 4.1 that

$$\bar{P}_{\bar{\gamma}} = P_\gamma \otimes_{R\tau} P'_{\gamma'} = \bar{P}_{\tilde{\gamma}}\,.$$

Let $\tau = (\delta, \beta + 2R)$; then (cf. Definition 3.3) the R-endomorphisms $T_\beta(\bar{\gamma})$, $T_\beta(\tilde{\gamma})$ of P coincide, since they represent multiplication by σ_β in the coinciding $R\tau$-modules $\bar{P}_{\bar{\gamma}}$ and $\bar{P}_{\tilde{\gamma}}$ with underlying R-module $\bar{P}$.

By Proposition 3.2, Corollary 1, we have

$$\begin{aligned} T_\beta(\tilde{\gamma})E_1 &= -\tfrac{1}{2}(B + \beta)E_1 + AE_2\,, \\ T_\beta(\tilde{\gamma})E_2 &= -CE_1 + \tfrac{1}{2}(B - \beta)E_2\,. \end{aligned} \tag{32}$$

We have

$$\bar{\epsilon} = u_0E_1 \wedge E_2$$

for some unit u_0 in R, and there exist $\bar{A}$, $\bar{B}$, $\bar{C}$ in R such that

$$\bar{q}(x_1E_1 + x_2E_2) = \bar{A}x_1^2 + \bar{B}x_1x_2 + \bar{C}x_2^2 \qquad (x_1\,,\ x_2 \in R).$$

Noting that with

$$\bar{E}_1 = u_0E_1\,, \qquad \bar{E}_2 = E_2\,,$$

we have $\bar{E}_1 \wedge \bar{E}_2 = \bar{\epsilon}$ and

$$\bar{q}(x_1\bar{E}_1 + x_2\bar{E}_2) = (\bar{A}u_0^2)x_1^2 + (\bar{B}u_0)x_1x_2 + \bar{C}x_2^2 \qquad (x_1\,,\ x_2 \in R)$$

we may again apply Proposition 3.2, Corollary 1 to obtain

$$\begin{aligned} T_\beta(\bar{\gamma})\bar{E}_1 &= -\tfrac{1}{2}(Bu_0 + \beta)\bar{E}_1 + Au_0^2\bar{E}_2\,, \\ T_\beta(\bar{\gamma})\bar{E}_2 &= -C\bar{E}_1 + \tfrac{1}{2}(Bu_0 - \beta)\bar{E}_2\,, \end{aligned}$$

i.e.,

$$\begin{aligned} T_\beta(\bar{\gamma})E_1 &= -\tfrac{1}{2}(\bar{B}u_0 + \beta)E_1 + \bar{A}u_0E_2\,, \\ T_\beta(\bar{\gamma})E_2 &= -\bar{C}u_0E_1 + \tfrac{1}{2}(\bar{B}u_0 - \beta)E_2\,. \end{aligned} \tag{33}$$

Since, as previous observed, $T_\beta(\bar\gamma) = T_\beta(\tilde\gamma)$, comparison of (32) and (33) shows that

$$A = \bar A u_0\,, \quad B = \bar B u_0\,, \quad C = \bar C u_0$$

whence

$$\tilde q = u_0 \bar q,$$
$$\operatorname{div}\bar\gamma = R\bar A + R\bar B + R\bar C = RA + RB + RC = \operatorname{div}\tilde\gamma.$$

By Theorems 1.16 and 2.6,

$$\operatorname{div}\tilde\gamma = \operatorname{div}_R Q_\Sigma = (\operatorname{div}_R q_\Sigma)(\operatorname{div}_R q'_\Sigma) = (\operatorname{div}\gamma)(\operatorname{div}\gamma')$$

so that, as asserted,

$$\operatorname{div}\bar\gamma = (\operatorname{div}\gamma)(\operatorname{div}\gamma').$$

Since both $\bar\gamma$ and $\tilde\gamma$ satisfy condition (iii) of Definition 4.1 with respect to γ and γ', we have (for all p in P, p' in P')

$$q(p)q'(p') = \tilde q(p \otimes_{R\tau} p') = u_0\bar q(p \otimes_{R\tau} p') = u_0 q(p)q'(p')$$

whence $1 - u_0$ annihilates all such products $q(p)\,q(p')$, and so annihilates the ideal

$$(\operatorname{div}\gamma)(\operatorname{div}\gamma') = \operatorname{div}\bar\gamma$$

which they generated over R. Thus, $(1 - u_0)\,\bar q(\bar p) = 0$ for all $\bar p$ in $\bar P$, so

$$\tilde q = u_0\bar q = \bar q.$$

It follows that, $\bar\gamma_1$ being any other semi-composite of γ and γ', there exists a unit u_1 in R such that $1 - u_1$ annihilates $\operatorname{div}\bar\gamma = \operatorname{div}\tilde\gamma$ (i.e., with u_1 in M) and such that $\bar\gamma_1 = (\bar P, u_1\,, \bar\epsilon, \bar q)$; then $u = u_0^{-1}u_1$ is in M and $\bar\gamma_1 = (\bar P, u\bar\epsilon, \bar q)$.

Conversely, if $u \in M$ and $\bar\gamma_1 = (\bar P, u\bar\epsilon, \bar q)$, then $\bar\gamma_1 = (\bar P, u_1\bar\epsilon, \tilde q)$, where $u_1 = uu_0$ is a unit in R such that $1 - u$ annihilates $\operatorname{div}\bar\gamma = \operatorname{div}\tilde\gamma$, i.e., such that

$$A = Au_1\,, \quad B = Bu_1\,, \quad C = Cu_1\,.$$

We may run the preceding argument backwards to show that $\bar\gamma_1$ satisfies conditions (ii) and (iii) of Definition 4.1 with respect to γ and γ' (since $\tilde\gamma$ does); to see that it also satisfies condition (i), i.e., that $\bar\gamma_1$ is of type τ, we need only note that $\bar\gamma_1$ is represented by the numerical form

$$[Au_1^2, Bu_1\,, C]^L = [A, B, C]^L$$

with respect to the properly oriented free basis $\{u_1E_1\,, E_2\}$. Hence, $\bar\gamma_1$ is also a semi-composite of γ and γ'. This completes the proof of the theorem in the special case in which R is quasi-local.

We now drop the assumption that R is quasi-local. $\operatorname{div}\bar{\gamma} = (\operatorname{div}\gamma)(\operatorname{div}\gamma')$ remains valid (as follows immediately from its validity in every localization, using Lemma 1.11(ii)). We are thus done if we prove the following statement:

(A) *A form* $\bar{\gamma}_1 = (\bar{P}, \bar{\epsilon}_1, \bar{q})$ *over* R *is a semi-composite of* γ *and* γ' *if and only if*: $\bar{q}_1 = \bar{q}$ *and, for some* u *in* M, $\bar{\epsilon}_1 = u\bar{\epsilon}$.

In order to reduce to the quasi-local case just treated, we begin by noting that the statement:

(C_1) *There exists a unit* u *in* R *such that* $u\bar{\epsilon} = \bar{\epsilon}_1$ *and* $1 - u$ *annihilates* $\operatorname{div}\bar{\gamma}$

is equivalent (since ϵ and ϵ_1 are R-orientations of (P) to the statement

(C_2) *There exists an element* u *in* R *satisfying*: $u\bar{\epsilon} = \bar{\epsilon}_1$, $ui = 0$ *for all* i *in* $\operatorname{div}\bar{\gamma}$.

Since $\operatorname{div}\gamma$ is finitely generated over R by Proposition 1.18, and using the well-known fact that a finite system of linear equations over R is solvable over R if and only if it is locally solvable at every maximal ideal of R, we see that (C_2) is equivalent to the following statement:

(C_3) *For every maximal ideal* M *of* R *there exists an element* u_M *in* R_M *satisfying*: $u_M\bar{\epsilon}_M = (\bar{\epsilon}_1)_M$, $u_M i_M = 0$ *for all* i *in* $\operatorname{div}\bar{\gamma}$.

This is, in turn, equivalent (by Lemma 1.11(ii)) to the statement:

(C_4) *For every maximal ideal* M *of* R, *there exists a unit* u_M *in* R_M *such that*: $u_M\bar{\epsilon}_M = (\bar{\epsilon}_1)_M$ *and* $1 - u_M$ *annihilates* $\operatorname{div}(\bar{\gamma}_M)$.

Using the equivalence of (C_1) and (C_4) together with Theorem 4.7, it is now straightforward to deduce the truth of (A) for R from its truth for every localization R_M (M a maximal ideal of R).

COROLLARY 1. *If two forms* γ *and* γ' *over* R *possess a semi-composite, then* γ *and* γ' *are composable if and only if*: u *a unit in* R *such that* $1 - u$ *annihilates* $(\operatorname{div}\gamma)(\operatorname{div}\gamma') \Rightarrow u = 1$.

COROLLARY 2. *If two primitive forms* γ *and* γ' *over* R *possess a semi-composite* $\bar{\gamma}$, *then* $\bar{\gamma}$ *is the composite of* γ *and* γ'.

Proof. $(\operatorname{div}\gamma)(\operatorname{div}\gamma') = R$; now apply Corollary 1.

COROLLARY 3. *If two forms* γ *and* γ' *over* R *with the same discriminant* δ *have a semi-composite* $\bar{\gamma}$, *and if* δ *is not a zero-divisor in* R, *then* $\bar{\gamma}$ *is a composite of* γ *and* γ'.

Proof. If $1 - u$ annihilates $(\operatorname{div}\gamma)(\operatorname{div}\gamma')$, then it annihilates $(\operatorname{div}\gamma)^2(\operatorname{div}\gamma')^2$, which by Proposition 1.12 contains $\delta(\gamma)\,\delta(\gamma') = \delta^2$; since δ is not a zero-divisor in R, this implies $u = 1$.

Remark. Consider the following property of the form γ: "There is no unit $u \neq 1$ in R such that $1 - u$ annihilates $\operatorname{div}\gamma$." This property does not behave well under localization; in consequence, it is possible for two forms γ and γ' to be composable, while, for some maximal ideal M of R, γ_M and γ'_M are not composable. (Things behave well in the other direction, "local to global," however; cf. Theorem 4.10 below.)

This difficulty can only arise when the common discriminant of γ and γ' is a zero-divisor and at least one of γ and γ' is not primitive (as is easy to show). Thus, fortunately, this point will not affect the construction of the generalized Gaussian composition groups (even when the discriminant is a zero-divisor) since this construction only involves primitive forms.

EXAMPLE. Let k be a field of characteristic $\neq 2$, and let

$$R = k[x, y]/(xy) = k[\bar{x}, \bar{y}] \qquad (\bar{x}, \bar{y} \text{ the residue classes of } x, y \bmod xy).$$

Also, let

$$\gamma = \left(R^2, \binom{1}{0} \wedge \binom{0}{1}, [\bar{y}, 0, \bar{y}]^L\right), \qquad \gamma' = \left(R^2, \binom{1}{0} \wedge \binom{0}{1}, [1, 0, \bar{y}^2]^L\right),$$

$$M = R(\bar{x} + 1) + R\bar{y}.$$

Since $[\bar{y}, 0, \bar{y}]^L$ and $[1, 0, \bar{y}^2]^L$ possess a Gaussian composite over R, as may be seen by considering

$$\Sigma = \begin{pmatrix} 1, & 0, & 0, & -\bar{y} \\ 0, & \bar{y}, & 1, & 0 \end{pmatrix}$$

(cf. Example 5 in Section 2) it follows that the forms γ and γ' possess a semi-composite, and hence are composable by the preceding Corollary 1. (Note that $(\operatorname{div}\gamma)\,(\operatorname{div}\gamma') = R\bar{y}$ and that, as is easily proved, all units of R lie in k.) M is a maximal ideal of R, and $\bar{x}_M$ annihilates $(\operatorname{div}\gamma_M)(\operatorname{div}\gamma'_M) = R\bar{y}_M$; since it is readily seen that $1 - \bar{x}_M = u$ is a unit of R_M which is not 1, γ_M, and γ'_M are not composable.

The proof of Theorem 4.11 below will require some elementary scheme-theoretical methods, in order to pass from the local to the general case, and in this connection we shall adopt the following standard notation:

If $r \in R$ and E is an R-module, then $D(r)$ will denote the open subset

$$\{M \text{ in Spec } R\colon r \notin M\}$$

of Spec R, while R_r and E_r will denote $S^{-1}R$ and $S^{-1}E$, respectively, where S is the multiplicatively closed subset of R consisting of all nonnegative integral powers of r. If $u \in E_r$, $M \in D(r)$, we denote by u_M the image of u under the canonical composite

$$E_r \to (E_r)_{MR_r} \approx E_M$$

and, in general, we shall identify $(E_r)_{MR_r}$ with E_M. Expressions such as γ_r, $\epsilon_{(r)}$, τ_r will be interpreted as meaning γ_f, $\epsilon_{(f)}$, $q_{(f)}$, τ_f, where f is the canonical ring-homomorphism $R \to R_r$, and we shall identify $(\gamma_r)_{MR_r}$ with γ_M, $(\epsilon_{(r)})_{(MR_r)}$ with $\epsilon_{(M)}$, etc., if $M \in D(r)$.

LEMMA 4.9. *Let $\gamma = (P, \epsilon, q)$ and $\gamma' = (P', \epsilon', q')$ be forms over R, and let M be a a prime ideal of R. If the forms γ_M and γ'_M over R_M possess a semi-composite, then for some r in $R - M$ (i.e., with $M \in D(r)$), the forms γ_r and γ'_r over R_r possess a semi-composite.*

Proof. Suppose that γ_M, γ'_M are represented, respectively, by $[a_1(M), a_2(M), a_3(M)]^L$, $[a'_1(M), a'_2(M), a'_3(M)]^L$ with respect to the properly oriented free bases $\{e_1(M), e_2(M)\}$, $\{e'_1(M), e'_2(M)\}$, respectively, for P_M, P'_M over R_M (cf. Definition 1.11). This assertion is exactly equivalent to the following set of equations:

$$e_1(M) \wedge e_2(M) = \epsilon_{(M)}, \qquad e'_1(M) \wedge e'_2(M) = \epsilon'_{(M)}, \tag{34}$$

$$q_{(M)}(e_1(M)) = a_1(M), \qquad q'_{(M)}(e'_1(M)) = a'_1(M), \tag{35}$$

$$q_{(M)}(e_2(M)) = a_3(M), \qquad q'_{(M)}(e'_2(M)) = a'_3(M), \tag{36}$$

$$q_{(M)}(e_1(M) + e_2(M)) = a_1(M) + a_2(M) + a_3(M), \tag{37}$$

and

$$q'_{(M)}(e'_1(M) + e'_2(M)) = a'_1(M) + a'_2(M) + a'_3(M).$$

It follows from Theorem 4.6 that

$$[a_1(M), a_2(M), a_3(M)]^L \quad \text{and} \quad [a'_1(M), a'_2(M), a'_3(M)]^L$$

possess a Gaussian composite over R_M. Again expressing ourselves in terms of explicit equations, we see that this fact is equivalent to the following assertion (cf. Definition 2.4):

There exist, in R_M, $m_i(M)$ and $n_i(M)$ $(0 \leqslant i \leqslant 3)$ and $e_{ij}(M)$ $(0 \leqslant i < j \leqslant 3)$ such that

$$a_1(M) = m_0(M)n_1(M) - m_1(M)n_0(M), \tag{38}$$

$$a_2(M) = m_0(M)n_3(M) - m_3(M)n_0(M) - m_1(M)n_2(M) + m_2(M)n_1(M), \tag{39}$$

$$a_3(M) = m_2(M)\, n_3(M) - m_3(M)\, n_2(M), \tag{40}$$

$$a_1'(M) = m_0(M)\, n_2(M) - m_2(M)\, n_0(M), \tag{41}$$

$$a_2'(M) = m_0(M)\, n_3(M) - m_3(M)\, n_0(M) + m_1(M)\, n_2(M) - m_2(M)\, n_1(M), \tag{42}$$

$$a_3'(M) = m_1(M)\, n_3(M) - m_3(M)\, n_1(M),$$

and

$$\sum_{0 \leqslant i < j \leqslant 3} e_{ij}(M)\,[m_i(M)\, n_j(M) - m_j(M)\, n_i(M)] = 1. \tag{44}$$

Let us denote by $\mathscr{o}$, $\mathscr{P}$, $\mathscr{P}'$, $\mathscr{L}$, $\mathscr{L}'$ the sheaves over Spec R associated (as in [00, Chap. 1, Sect. 1.3]) with the R-modules R, P, P', $\Lambda^2 P$, $\Lambda^2 P'$, respectively. For every r in R we shall identify, in the standard way (cf. [00, Chap. 1, Proposition 1.3.6, Theorem 1.3.7]) the sections of $\mathscr{o}$, $\mathscr{P}$, etc., over $D(r)$ with the elements, respectively, of R_r, P_r, etc.

There are isomorphisms

$$\begin{aligned} i_r &: \mathscr{L}(D(r)) = (\Lambda_R{}^2 P)_r \approx \Lambda^2_{R_r}(P_r), \qquad (p \wedge p')_r \mapsto p_r \wedge p_r' \\ i_M &: \mathscr{L}_M = (\Lambda_R{}^2 P)_M \approx \Lambda^2_{R_M}(P_M), \qquad (p \wedge p')_M \mapsto p_M \wedge p_M' \end{aligned} \tag{45}$$

which we shall regard as identifications; and similarly for P'.

Note that, for any

$$\hat{e} = e_r/r^m, \qquad \hat{f} = f_r/r^n$$

in P_r (where e, f are in P) the map

$$N \mapsto \hat{e}_N \wedge \hat{f}_N = (e \wedge f)_N/r^m\bar{p}^n \qquad (N \text{ in } D(R))$$

is a section of $\mathscr{L}$ over $D(r)$, and the map

$$N \to q_{(N)}(\hat{e}_N) = (q(e))_N/r^{2m} \qquad (N \text{ in } D(r))$$

is a section of $\mathscr{o}$ over $D(r)$; in this sense, Λ and q are continuous operations in the sheaves involved. Of course, a similar observation holds for P'.

We may find a basic open neighborhood $D(s)$ of M in Spec R (s in R) and sections over $D(s)$

$$\begin{aligned} &e_i(s) \text{ of } \mathscr{P},\ e_i'(s) \text{ of } \mathscr{P}' && (i = 1, 2), \\ &a_i(s),\ a_i'(s) \text{ of } \mathscr{o} && (i = 1, 2, 3), \\ &m_i(s),\ n_i(s) \text{ of } \mathscr{o} && (0 \leqslant i \leqslant 3), \\ &e_{ij}(s) \text{ of } \mathscr{o} && (0 \leqslant i < j \leqslant 3), \end{aligned} \tag{*}$$

which coincide, at M, with $e_i(M)$, $e_i'(M)$,..., $e_{ij}(M)$, respectively. It follows from the discussion in the paragraph preceding this one that, if we replace M by s in Eqs. (34) through (44), then each side of each of the resulting equations is a section in the relevant scheme ($\mathscr{L}$ or $\mathscr{L}'$ for (34), $\mathscr{o}$ for the rest; note that $\epsilon_{(s)}$ is a section of $\mathscr{L}$ over $D(s)$ by the identifications of (45)). Since an equation between sections which holds at a point, also holds in a neighborhood of that point, it follows that there exists r in R such that:

$M \in D(r) \subseteq D(s)$, and such that, if we denote by $e_i(r)$, $e_i'(r)$,..., $e_{ij}(r)$ the restrictions to $D(r)$ of the sections (*) listed above, then (34) through (44) still hold upon replacing M by r.

We now view $e_1(r)$ and $e_2(r)$ as elements of P_r, $e_1'(r)$ and $e_2'(r)$ as elements of P_r', and $a_1(r)$,..., $e_{23}(r)$ as elements of R_r; of course, this shift in viewpoint does not change the fact that (34) through (44) hold with M replaced by r. Since (cf. (34)) $e_i(r) \wedge e_2(r) = \epsilon_{(r)}$, it follows from Proposition 1.10 that P_r is free over R_r on $\{e_1(r), e_2(r)\}$, and similarly for P_r'. Thus, (34) through (37) (with M replaced by r) show that γ_r is represented by $[a_1(r), a_2(r), a_3(r)]^L$ with respect to the properly oriented free basis $\{e_1(r), e_2(r)\}$, and γ_r' is represented by $[a_1'(r), a_2'(r), a_3'(r)]^L$ with respect to the properly oriented free basis $\{e_1'(r), e_2'(r)\}$. Equations (38) through (44) (with M replaced by r) show that the numerical forms

$$[a_1(r), a_2(r), a_3(r)]^L \qquad \text{and} \qquad [a_1'(r), a_2'(r), a_3'(r)]^L$$

over R_r, associated with γ_r and γ_r', respectively, possess a Gaussian composite over R. By Theorem 4.6, γ_r and γ_r' possess a semi-composite.

THEOREM 4.10. *Let γ and γ' be forms over R such that γ_M and γ_M' are composable for every prime ideal M of R; then γ and γ' are composable.*

Remark. Theorem 4.10 remains true with "prime" replaced by "maximal"; this is not difficult to show once it is noted that if R is quasi-local, and I is any ideal of R, then the criterion of Corollary 1 to Theorem 4.8:

"*u a unit of R such that $(I - u)I = 0 \Rightarrow u = 1$*"

is satisfied if and only if the only element of R which annihilates I is 0. (Proposition 1.18 should also be recalled.)

Proof of Theorem 4.10. Let

$$\gamma = (P, \epsilon, q), \qquad \gamma' = (P', \epsilon', q').$$

Let τ and τ' be the form-types of γ, γ', respectively.

By hypothesis, γ_M and γ'_M are composable for every prime ideal M of R; let

$$\gamma_M\gamma'_M = (\hat{P}(M), \hat{\epsilon}(M), \hat{q}(M)).$$

By (i) of Definition 4.1, γ_M and γ'_M are of the same form-type; hence, by Lemma 1.17(ii), $\tau_M = \tau'_M$; since this is true for every prime ideal M of R, $\tau = \tau'$.

By (ii) of Definition 4.1, $\hat{P}(M)$ is the R_M-module underlying the $R_M\tau_M$-module

$$(P_M)_{\gamma_M} \otimes_{R_M\tau_M} (P'_M)_{\gamma'_M}.$$

We must construct a composite of γ and γ'; at least we know that its underlying R-module must be that underlying the $R\tau$-module $P_\gamma \otimes_{R\tau} P'_{\gamma'}$, whose underlying R-module we denote by $\bar{P}$.

Recall the R_M-isomorphism

$$\psi^M\colon \bar{P}_M = (P_\gamma \otimes_{R\tau} P'_{\gamma'})_M \approx (P_M)_{\gamma_M} \otimes_{R_M\tau_M} (P'_M)_{\gamma'_M} = \hat{P}(M)$$

defined in the statement of Theorem 4.7. Let us use this to pull $\gamma_M\gamma'_M$ back from $\hat{P}(M)$ to a form

$$\bar{\gamma}(M) = (\bar{P}_M, \bar{\epsilon}(M), \bar{q}(M) = [(\psi^M)^{-1}]_*(\gamma_M\gamma'_M) \tag{46}$$

on $\bar{P}_M$.

Claim. The maps

$$\operatorname{Spec} R \to \mathscr{L},\ M \mapsto \bar{\epsilon}(M),$$

and

$$\operatorname{Spec} R \to \mathscr{G},\ M \mapsto \bar{q}(M),$$

are sections of the sheaves $\mathscr{L}$ and $\mathscr{G}$ over Spec R associated, respectively, with the R-modules $\Lambda^2\bar{P}$ and $LQ_R(\bar{P})$.

(Note: In connection with these two sheaves, we shall regard as identifications the isomorphisms of (45) with P replaced by $\bar{P}$) and the isomorphisms

$$\begin{aligned} \mathscr{G}(D(r)) = (LQ_R(\bar{P}))_r &\approx LQ_{R_r}(P_r), \qquad q_r \mapsto q_{(r)}, \\ \mathscr{G}_M = (LQ_R(\bar{P}))_M &\approx LQ_{R_M}(\bar{P}_M), \qquad q_M \mapsto q_{(M)}, \end{aligned} \tag{47}$$

of Proposition 1.2(iv).

To justify the preceding claim, it suffices to show that, given any M in Spec R, there exist r in $R - M$, $\bar{\epsilon}(r)$ in $\mathscr{L}(D(r)) = (\Lambda^2(P))_r$, and $\bar{q}(r)$ in $\mathscr{Q}(D(r)) = (LQ_R(P))_r$, such that for every N in $D(r)$,

$$\bar{\epsilon}(N) = (\bar{\epsilon}(r))_N, \qquad \bar{q}(N) = (\bar{q}(r))_N. \tag{48}$$

Let $M \in \text{Spec } R$. By Lemma 4.10, there exists an r in $R - M$ such that γ_r and γ'_r possess a semi-composite $\hat{\gamma}(r)$; let

$$\hat{\gamma}(r) = (\hat{P}(r), \hat{\epsilon}(r), \hat{q}(r))$$

and note that $\hat{P}(r)$ is the R_r-module underlying

$$(P_r)_{\gamma_r} \otimes_{R_r\tau_r} (P'_r)_{\gamma'_r}.$$

By Theorem 4.1 there are the two following isomorphisms, analogous to ψ^M, and arising, respectively, from the canonical ring-homomorphisms $R \to R_r$ and $R_r \to R_N$:

$$\psi^r\colon \bar{P}_r \approx \hat{P}(r), \qquad (p \otimes_{R\tau} p')_r \mapsto p_r \otimes_{R_r\tau_r} p'_r,$$

$$\psi^{r,N}\colon [\hat{P}(r)]_N \approx P(N), \qquad (p_r \otimes_{R_r\tau_r} p'_r)_N \to p_N \otimes_{R_N\tau_N} p'_N$$

(p in P, p' in P').

Recall that we are identifying $\bar{P}_N$ with $(\bar{P}_r)_N$, and note the commuting diagram

$$\begin{array}{ccc} \bar{P}_N & \xrightarrow{[\psi^r]_N} & [\hat{P}(r)]_N \\ & {\scriptstyle \psi^N} \searrow & \downarrow {\scriptstyle \psi^{r,N}} \\ & & \hat{P}(N) \end{array}$$

We now show that (48) holds if we set

$$[(\psi^r)^{-1}]_* \hat{\gamma}(r) = (\bar{P}_r, \bar{\epsilon}(r), \bar{q}(r)) = \bar{\gamma}(r).$$

First note that ψ^r is a proper R_r-equivalence from $\bar{\gamma}(r)$ to $\hat{\gamma}(r)$ (cf. Proposition 1.8). $[\psi^r]_N$ is then a proper R_N-equivalence from $[\bar{\gamma}(r)]_N$ to $[\hat{\gamma}(r)]_N$, while Theorem 4.1 shows that $\psi^{r,N}$ is a proper R_N-equivalence from $[\hat{\gamma}(r)]_N$ to a semi-composite of γ_N and γ'_N, i.e., to the unique semi-composite $\gamma_N\gamma'_N$. Thus, $\psi^N = \psi^{r,N} \circ (\psi^r)_N$ is a proper R_N-equivalence from $[\bar{\gamma}(r)]_N$ to $\gamma_N\gamma'_N$, whence

$$\bar{\gamma}(N) = [(\psi^N)^{-1}]_* (\gamma_N\gamma'_N) = [\bar{\gamma}(r)]_N,$$

i.e.,

$$(\bar{P}_N, \bar{\epsilon}(N), \bar{q}(N)) = (\bar{P}_N, [\bar{\epsilon}(r)]_N, [\bar{q}(r)]_N),$$

so (48) holds, and the claim is justified.

By [24, Chap. 1, Theorem 1.3.7] it follows that there exist $\bar{\epsilon}$ in Λ^2 and $\bar{q}$ in $LQ_R(P)$ such that, for every prime ideal M of R,

$$\bar{\epsilon}_M = \bar{\epsilon}(M), \qquad \bar{q}_M = \bar{q}(M).$$

Let

$$\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q}).$$

For every prime ideal M of R, we have (cf. (46))

$$\bar{\gamma}_M = \bar{\gamma}(M) = [(\psi^M)^{-1}]_* (\gamma_M \gamma'_M),$$

i.e., $(\psi^M)_*(\bar{\gamma}_M)$ is the composite of γ_M and γ^M, and it follows from Theorem 4.7 that $\bar{\gamma}$ is a semi-composite of γ and γ'.

If $\bar{\gamma}$ were not the unique semi-composite of γ and γ', then, by Theorem 4.8, there would be a unit u in R, distinct from 1, such that $1 - u$ annihilates $\operatorname{div} \bar{\gamma}$. There then exists a prime ideal M of R such that $(1 - u)_M \neq 0$; then u_M is a unit of R_M, distinct from 1, such that $1 - u_M$ annihilates

$$(\operatorname{div} \bar{\gamma})_M R_M = ((\operatorname{div} \gamma)(\operatorname{div} \gamma'))_M R_M = (\operatorname{div} \gamma_M)(\operatorname{div} \gamma'_M)$$

(cf. Lemma 1.11(ii) and Theorem 4.8) and, again by Theorem 4.8, this contradicts the hypothesis that γ_M and γ'_M are composable. Thus, $\bar{\gamma}$ is the composite of γ and γ', which completes the proof.

THEOREM 4.11. *Two forms γ and γ' over R of the same form-type are composable if they satisfy either of the two following conditions:*

(A) *γ and γ' are primitive.*

(B) *γ and γ' are comaximal, and their common discriminant is not a zero-divisor in R.*

Let γ and γ' satisfy (A) or (B), and let M be a prime ideal of R; we are done (by Theorem 4.10) if we prove that γ_M and γ'_M are composable. γ_M and γ'_M themselves satisfy (A) or (B); thus, (by Corollaries 1 and 2 to Theorem 4.8) it suffices to show that γ_M and γ'_M possess a semi-composite. γ_M and γ'_M are free, and we may assume they are associated, respectively, with the numerical forms

$$q = [a, b, c]^L, \qquad q' = [a', b', c']^L$$

over R_M. Thus, by Theorem 4.5, the proof of the theorem will be complete if we show that q and q' possess a Gaussian composite over R_M.

Since γ_M and γ'_M satisfy (A) or (B), they are comaximal and of the same type. Hence, the numerical forms q and q' over R_M are comaximal and have the same discriminant and parity. Let

$$d_{01} = a, \quad d_{02} = a', \quad d_{03} = \tfrac{1}{2}(b' + b), \quad d_{12} = \tfrac{1}{2}(b' - b), \quad d_{13} = c', \quad d_{23} = c.$$

Note that the expressions for d_{03} and d_{12} make sense because the numerical forms q and q' have the same parity, i.e.,

$$b + 2R_M = b' + 2R_M$$

and 2 is not a zero-divisor on R_M. Note also that these six d_{ij} generate the unit ideal in R_M, since the numerical forms q and q' are comaximal, i.e.,

$$R_M = R_M a + R_M b + R_M c + R_M a' + R_M b' + R_M c'$$

and since

$$b = d_{03} - d_{12}, \qquad b' = d_{03} + d_{12}.$$

To show that the numerical forms q and q' possess a Gaussian composite over R_M, it suffices to show there exists a 2×4 matrix

$$\Sigma = \begin{pmatrix} m_0, & m_1, & m_2, & m_3 \\ n_0, & n_1, & n_2, & n_3 \end{pmatrix}$$

over R_M such that

$$d_{ij} = m_i n_j - m_j n_i \qquad (0 \leqslant i < j \leqslant 3)$$

for then (cf. Definition 2.4) it follows that Σ is unimodular over R_M and that $q = [a, b, c]^L = q_\Sigma$, $q' = q'_\Sigma$.

Let F be an R_M-module, free on $\{f_0, f_1, f_2, f_3\}$ over R_M, and let ω denote the element

$$\omega = \sum_{0 \leqslant i < j \leqslant 3} d_{ij} f_i \wedge f_j$$

in $\Lambda^2 F$. Using the terminology defined in Section 1 of [33], ω is a "Plucker" and "unimodular" element of $\Lambda^2 F$ (the former because the numerical forms q and q' have the same discriminant, i.e.,

$$b^2 - 4ac = b'^2 - 4a'c',$$

whence,

$$d_{01} d_{23} - d_{02} d_{13} + d_{03} d_{12} = 0;$$

the latter because, as we have seen, the d_{ij} generate the unit ideal in R). From this, and the fact projective R_M-modules are free, it follows from [33, Theorem 1.1, Corollary 2] that there exist

$$u = \sum_0^3 m_i f_i, \; v = \sum_0^3 n_i f_i \qquad (m_i, n_i \text{ in } R_M)$$

in F such that $\omega = u \wedge v$, i.e., such that $d_{ij} = m_i n_j - m_j n_i$. Thus, the numerical forms q and q' possess a Gaussian composite over R_M, which completes the proof of Theorem 4.11.

LEMMA 4.12. *If $\bar{\gamma}$ is a semi-composite of the forms γ and γ' over R, and if T, T' are proper equivalences over R from γ to γ_1 and γ' to γ_1', respectively, then there is a natural proper equivalence $T \otimes_{R\tau} T'$ over R from $\bar{\gamma}$ to a semi-composite of γ and γ'.*

Proof. Straightforward, using Def. 4.1 and Prop. 3.3.

COROLLARY. *If γ and γ' are composable, then any form in* cls γ *is composable with any form in* cls γ', *and the set of all such composites is contained in a single form-class.*

DEFINITION 4.2. Let Γ and Γ'' be two form-classes over R. Γ will be called *composable* with Γ'' if one (hence every) form in Γ is composable with one (hence every) form in Γ'', in which case the *composite* $\Gamma\Gamma''$ iof Γ and Γ'' is defined to be the form-class containing all composites $\gamma\gamma'$ with γ in Γ and γ' in Γ''.

It follows from Theorem 4.11 that any two form-classes in $PC_R(\tau)$ are composable. If Γ and Γ'' are in $PC_R(\tau)$, then $\Gamma\Gamma''$ is of type τ (Definition 4.1(i)) and is primitive by Theorem 4.8, i.e., $\Gamma\Gamma''$ is again in $PC_R(\tau)$. The remainder of this paper will be devoted to proving that the binary operation thus obtained on $PC_R(\tau)$ is a commutative group operation. We begin with the commutative law:

THEOREM 4.13. *If $\bar{\gamma}$ is a semi-composite of the forms $\gamma = (P, \epsilon, q)$ and $\gamma' = (P', \epsilon', q')$ of type τ over R, then*

$$P_\gamma \otimes_{R\tau} (P')_{\gamma'} \to (P')_{\gamma'} \otimes_{R\tau} P_\gamma, \qquad p \times p' \mapsto p' \times p$$

is a proper equivalence over R from γ to a semi-composite of γ' and γ. If the form-class Γ over R is composable with the form-class Γ'', then also Γ'' is composable with Γ, and $\Gamma\Gamma'' = \Gamma''\Gamma$.

Proof. Straightforward.

The following lemma will be utilized in the proof of the associative law.

LEMMA 4.14. *If R is quasi-local, and the forms $\gamma = (P, \epsilon, q)$ and $\gamma' = (P', \epsilon', q')$ of type τ over R have the semi-composite $\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q})$, then every element in $\bar{P} = P_\gamma \otimes_{R\tau} (P')_{\gamma'}$ is of the form $p \otimes_{R\tau} p'$ with p in P, p' in P'.*

Proof. Since R is quasi-local, P and P' are free over R, say on $\{e_1, e_2\}$ and $\{e_1', e_2'\}$, respectively, with $e_1 \wedge e_2) = \epsilon$ and $e_1' \wedge e_2' = \epsilon'$.

There then exist a, b, c, a', b', and c' in R such that

$$q(x_1e_1 + x_2e_2) = ax_1^2 + bx_1x_2 + cx_2^2,\ q'(x_1e_1' + x_2e_2') = a'x_1^2 + b'x_1x_2 + c'x_2^2$$

for all x_1 and x_2 in R.

Since also $\bar{P}$ is free over R, it follows from Theorem 4.6 that there exists a unimodular 2×4 matrix

$$\Sigma = \begin{pmatrix} m_0, & m_1, & m_2, & m_3 \\ n_0, & n_1, & n_2, & n_3 \end{pmatrix}$$

over R such that $q_\Sigma = [a, b, c]^L$ and $q'_\Sigma = [a', b', c']^L$. We may now apply the Corollary to Theorem 4.5; thus, P has a free basis $\{E_1, E_2\}$ over R such that Eqs. (20) hold. Thus, we have for all x_1, x_2, x_1', and x_2' in R,

$$(x_1e_1 + x_2e_2) \otimes_{R\tau} (x_1'e_1 + x_2'e_2) = X_1E_1 + X_2E_2,$$

where

$$\begin{aligned} X_1 &= m_0x_1x_1' + m_1x_1x_2' + m_2x_2x_1' + m_3x_2x_2', \\ X_2 &= n_0x_1x_1' + n_1x_1x_2' + n_2x_2x_1' + n_2x_2x_2'. \end{aligned} \tag{49}$$

Accordingly, we are done if we show that Σ has the following property, which we shall call, property A: For all X_1 and X_2 in R, there exist x_1, x_2, x_1', x_2' in R satisfying (49). We now prove: Σ unimodular $\Rightarrow$ Σ has property A.

Since Σ is unimodular, its first row generates the unit ideal in R; since R is quasi-local, one of m_0, m_1, m_2, m_3 must thus be a unit in R. Interchanging x_1 and x_2 in (49), we see that

$$\begin{pmatrix} m_2, & m_3, & m_0, & m_1 \\ n_2, & n_3, & n_0, & n_1 \end{pmatrix}$$

has property A if and only if Σ does; similarly we see (interchanging x_1' and x_2') that

$$\begin{pmatrix} m_1, & m_0, & m_3, & m_2 \\ n_1, & n_0, & n_3, & n_2 \end{pmatrix}$$

has property A if and only if Σ does; combining the two preceding (commuting) operations,

$$\begin{pmatrix} m_3, & m_2, & m_1, & m_0 \\ n_3, & n_2, & n_1, & n_0 \end{pmatrix}$$

has property A if and only if Σ does. We may thus assume without loss of generality that m_0 is a unit in R. Replacing X by $m_0^{-1}X$ in (49), we may assume that $m_0 = 1$.

Replacing x_1 and x_1' by $x_1 + rx_2$ and $x_1' + r'x_2'$, respectively, in (49), with r and r' arbitrary elements of R, we see that

$$\begin{pmatrix} m_0\,,\ m_1 + r'm_0\,,\ m_2 + rm_0\,,\ m_3 + rr'm_0 + rm_1 + r'm_2 \\ n_0\,,\ n_1 + r'n_0\,,\ n_2 + rn_0\,,\ n_3 + rr'n_0 + rn_1 + r'n_2 \end{pmatrix}$$

has property A if and only if Σ does; note also that it is unimodular since Σ is. Since we may assume that $m_0 = 1$, it follows that we may then assume without loss of generality that also $m_1 = m_2 = 0$. Finally, replacing X_2 by $X_2 - n_0X_1$ in (49), we may also assume that $n_0 = 0$.

Thus, we have reduced to the case in which Σ is of the special form

$$\Sigma = \begin{pmatrix} 1, & 0, & 0, & m_3 \\ 0, & n_1\,, & n_2\,, & n_3 \end{pmatrix}$$

and it suffices to show that then, for all X_1 and X_2 in R there exist x_1, x_2, x_1' and x_2' in R satisfying the equations

$$\begin{aligned} X_1 &= x_1x_1' + m_3x_2x_2'\,, \\ X_2 &= n_1x_1x_2' + n_2x_2x_1' + n_3x_2x_2'\,. \end{aligned} \tag{49a}$$

Since Σ is unimodular, we have $R = Rn_1 + Rn_2 + Rn_3$, and since R is quasi-local, one of n_1, n_2, n_3 is a unit in R. If n_1 is a unit in R, then

$$x_1 = 1, \quad x_2 = 0, \quad x_1' = X_1\,, \quad x_2' = n_1^{-1}X_2$$

satisfy (49a). If n_2 is a unit in R, then

$$x_1 = X_1\,, \quad x_2 = n_2^{-1}X_2\,, \quad x_1' = 1, \quad x_2' = 0$$

satisfy (49a). Finally, if n_3 is a unit in R, we may reason as follows:

Clearly, we are done if we find x_1' and x_2' in R such that (49a), considered as equations in x_1 and x_2 :

$$\begin{aligned} X_1 &= x_1'x_1 + (m_3x_2')x_2\,, \\ X_2 &= (n_1x_2')x_1 + (n_2x_1' + n_3x_2')x_2 \end{aligned}$$

have a determinant

$$q_\Sigma'\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{vmatrix} x_1'\,, & m_3x_2' \\ n_1x_2'\,, & n_2x_1' + n_3x_2' \end{vmatrix} = n_2x_1'^2 + n_3x_1'x_2' - m_3n_1x_2'^2$$

which is a unit in R. Such x' and y' exist because the range $[n_2, n_3, -m_3 n_1^L]$ generates over R the ideal $\mathrm{div}_R q'_\Sigma$ which contains the unit n_3 (cf. proof of Proposition 1.16); since R is quasi-local, this range must contain a unit.

Remark. The preceding reduction of Σ to the special form

$$\begin{pmatrix} 1, & 0, & 0, & m_3 \\ 0, & n_1, & n_2, & n_3 \end{pmatrix}$$

may also be used to show that, for quasi-local rings, the method of united forms may be applied to compose any comaximal form-classes of the same type; this fact is, however, only an extremely special case of a result of Butts and Estes [9]. This reduction may also be used to give a very simple alternative proof, using localization, of Theorem 2.6.

We next prove that composition on $PC_R(\tau)$ is associative.

THEOREM 4.15. *Let $\gamma_i = (P_i, \epsilon_i, q_i)$ $(i = 1, 2, 3)$ be three primitive forms over R of the same type τ. Then the natural $R\tau$-isomorphism*

$$\phi\colon ((P_1)_{\gamma_1} \otimes_{R\tau} (P_2)_{\gamma_2}) \otimes_{R\tau} (P_3)_{\gamma_3} \approx (P_1)_{\gamma_1} \otimes_{R\tau} ((P_2)_{\gamma_2} \otimes_{R\tau} (P_3)_{\gamma_3})$$

is a proper equivalence over R from $(\gamma_1\gamma_2)\gamma_3$ to $\gamma_1(\gamma_2\gamma_3)$.

If $\Gamma_1, \Gamma_2, \Gamma_3$ lie in $PC_R(\tau)$, then

$$(\Gamma_1\Gamma_2)\Gamma_3 = \Gamma_1(\Gamma_2\Gamma_3).$$

Proof. We must verify that

$$\phi_*((\gamma_1\gamma_2)\gamma_3) = \gamma_1(\gamma_2\gamma_3).$$

We consider first the case that R is quasi-local. By Theorem 4.8, Corollary 2, it suffices to show that $\phi_*((\gamma_1\gamma_2)\gamma_3)$ is a semi-composite of γ_1 and $\gamma_2\gamma_3$, by verifying conditions (i), (ii), (iii) of Definition 4.1.

(Ad (i) Since by hypothesis γ_1, γ_2, and γ_3 are of type τ, so are $\gamma_1\gamma_2$, $\gamma_2\gamma_3$, $(\gamma_1\gamma_2)\gamma_3$, $\gamma_1(\gamma_2\gamma_3)$ and (by Lemma 1.17(i)) $\phi_*((\gamma_1\gamma_2)\gamma_3)$.

(Ad (ii) Let

$$\gamma_1\gamma_2 = (P_{12}, \epsilon_{12}, q_{12}),\ \gamma_2\gamma_3 = (P_{23}, \epsilon_{23}, q_{23}),\ (\gamma_1\gamma_2)\gamma_3 = (P', \epsilon', q'),$$
$$\phi_*((\gamma_1\gamma_2)\gamma_3) = \bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q})$$

then we must show that

$$\bar{P}_{\bar{\gamma}} = (P_1)_{\gamma_1} \otimes_{R\tau} (P_{23})_{\gamma_2\gamma_3}.$$

It follows from Definition 4.1 that

$$(P_{12})_{\gamma_1\gamma_2} = (P_1)_{\gamma_1} \otimes_{R\tau} (P_2)_{\gamma_2}\,,\ (P_{23})_{\gamma_2\gamma_3} = (P_2)_{\gamma_2} \otimes_{R\tau} (P_3)_{\gamma_3}\,,$$

$$(P')_{\gamma_1\gamma_2)\ \gamma_3} = (P_{12})_{\gamma_1\gamma_2} \otimes_{R\tau} (P_3)_{\gamma_3} = ((P_1)_{\gamma_1} \otimes_{R\tau} (P_2)_{\gamma_2}) \otimes_{R\tau} (P_3)_{\gamma_3}\,,$$

and what is to be shown may be written as

$$\bar{P}_{\bar{\gamma}} = (P_1)_{\gamma_1} \otimes_{R\tau} ((P_2)_{\gamma_2} \otimes_{R\tau} (P_3)_{\gamma_3}).$$

Now, ϕ is the natural $R\tau$-isomorphism

$$((P_1)_{\gamma_1} \otimes_{R\tau} (P_2)_{\gamma_2}) \otimes_{R\tau} (P_3)_{\gamma_3} \to (P_1)_{\gamma_1} \otimes_{R\tau} ((P_2)_{\gamma_2} \otimes_{R\tau} (P_3)_{\gamma_3}) \tag{50}$$

considered as an R-isomorphism from the R-module P' to the R-module $\bar{P}$. Since the $R\tau$-module structure on $(P')_{(\gamma_1\gamma_2)\gamma_3}$ is given by the left-hand side of (50), and since by Lemma 3.3, ϕ is an $R\tau$-module isomorphism from $(P')_{(\gamma_1\gamma_2)\gamma_3}$ to $\bar{P}_{\bar{\gamma}}$, it follows that the $R\tau$-module structure $\bar{P}_{\bar{\gamma}}$ is given by the right-hand side of (50), which is what we had to prove.

(Ad (iii) We retain the notation introduced in the proof of (ii). We must show that

$$\bar{q}(p_1 \otimes_{R\tau} p_{23}) = q_1(p_1)\, q_{23}(p_{23}) \tag{51}$$

holds for all p_1 in P_1 and p_{23} in $P_{23} = (P_2)_{\gamma_2} \otimes_{R\tau} (P_3)_{\gamma_3}$. Since we are assuming that R is quasi-local, it follows from Lemma 4.14 that there exist p_2 in P_2, p_3 in P_3 such that $p_{23} = p_2 \otimes_R p_3$, and (51) then follows from

$$\begin{aligned}
\bar{q}(p_1 \otimes_{R\tau} (p_2 \otimes_{R\tau} p_3)) &= q'(\phi^{-1}(p_1 \otimes_{R\tau} (p_2 \otimes_{R\tau} p_3)) \\
&= q'((p_1 \otimes_{R\tau} p_2) \otimes_{R\tau} p_3) \\
&= q_{12}(p_1 \otimes_{R\tau} p_2)\, q_3(p_2) \\
&= q_1(p_1)\, q_2(p_2)\, q_3(p_3) \\
&= q_1(p_1)\, q_{23}(p_2 \otimes_{R\tau} p_3).
\end{aligned}$$

This completes the proof of the theorem in the quasi-local case.

We now drop the hypothesis that R is quasi-local. Let M be any maximal ideal of R, and let $\mathscr{P}_i = ((P_i)_M)_{(\gamma_i)_M}$. We know the natural $R_M\tau_M$-isomorphism

$$\phi(M)\colon (\mathscr{P}_1 \times_{R_M\tau_M} \mathscr{P}_2) \times_{R_M\tau_M} \mathscr{P}_3 \approx \mathscr{P}_1 \times_{R_M\tau_M} (\mathscr{P}_2 \times_{R_M\tau_M} \mathscr{P}_3)$$

is a proper equivalence over R_M from $((\gamma_1)_M(\gamma_2)_M)(\gamma_3)_M$ to $(\gamma_1)_M((\gamma_2)_M(\gamma_3)_M)$. Consider the following diagram:

$$\begin{array}{ccc}
[(\gamma_1\gamma_2)\gamma_3]_M & \xrightarrow{\phi_M} & [\gamma_1(\gamma_2\gamma_3)]_M \\
\downarrow{\scriptstyle \psi^M_{12,3}} & & \downarrow{\scriptstyle \psi^M_{1,23}} \\
(\gamma_1\gamma_2)_M(\gamma_3)_M & & (\gamma_1)_M(\gamma_2\gamma_3)_M \\
\downarrow{\scriptstyle \psi^M_{12}\otimes \mathrm{Id}} & & \downarrow{\scriptstyle \mathrm{Id}\otimes\psi^M_{23}} \\
((\gamma_1)_M(\gamma_2)_M)(\gamma_3)_M & \xrightarrow{\phi(M)} & (\gamma_1)_M((\gamma_2)_M(\gamma_3)_M)
\end{array}$$

Here the various ψ^M are special cases of the map ψ in Theorem 4.1, with f the canonical map $R \to R/M$ (and, e.g., for $\psi^M_{12,3}$, with γ, γ' replaced by $\gamma_1\gamma_2$, γ_3, respectively). If we replace the various forms in this diagram by their underlying R_M-modules, we obtain a commuting diagram of modules and R_M-isomorphisms. Returning to the original diagram, we note that by Theorem 4.1 the vertical maps are all proper R_M-equivalences; also $\phi(M)$ is a proper R_M-equivalence. Hence, ϕ_M is a proper R_M-equivalence. Since this is so for all maximal ideals M of R, ϕ is a proper R-equivalence. This completes proof of associativity.

Our next theorem shows that $PC_R(\tau)$ has an identity element for composition, namely, cls $\iota(\tau)$ (cf. Definition 3.2).

THEOREM 4.16. *Let $\gamma = (P, \epsilon, q)$ be a form over R of type τ; then the $R\tau$-isomorphism*

$$I(\gamma)\colon P_\gamma \approx P_\gamma \otimes_{R\tau} R\tau, \qquad p \mapsto p \otimes 1$$

is a proper R-equivalence from γ to a semi-composite of γ and $\iota(\tau)$.

Proof. Let

$$(I_\gamma)_{*\gamma} = \hat{\gamma} = (\hat{P}, \hat{\epsilon}, \hat{q})$$

so that $\hat{P}$ is the R-module underlying $P_\gamma \otimes_{R\tau} R\tau$.

We must show that γ is a semi-composite of γ and $\iota(\tau)$; let us verify conditions (i), (ii), and (iii) of Definition 4.1.

(Ad (i) γ and hence the properly equivalent form $\hat{\gamma}$ are of type τ, as is $\iota(\tau)$.

(Ad (ii) We must show the $R\tau$-modules $\hat{P}_{\hat{\gamma}}$ and $P_\gamma \otimes_{R\tau} (R\tau)_{\iota(\tau)}$ coincide. By Corollary 2 to Proposition 3.2, this means we must show that (as $R\tau$-modules)

$$\hat{P}_{\hat{\gamma}} = P_\gamma \otimes_{R\tau} R\tau,$$

which follows immediately from the fact that, by Proposition 3.3, the proper R-equivalence

$$I_\gamma : P \to \hat{P}, \qquad p \mapsto p \otimes_{R\tau} 1$$

form γ to $\hat{\gamma}$ is an $R\tau$-isomorphism from P_γ to $\hat{P}_{\hat{\gamma}}$, as well as being an $R\tau$-isomorphism from P_γ to $P_\gamma \otimes_{R\tau} R\tau$.

(Ad (iii) By Proposition 3.2, Corollary 3, we have (for all p in P, s in R)

$$q(p)Nms = q(sp) = \hat{q}(I_\gamma(sp)) = \hat{q}(p \otimes_{R\tau} s).$$

LEMMA 4.17. *If $T: P \to P'$ is a proper equivalence over R from (P, ϵ, q) to (P', ϵ', q'), it is also a proper equivalence over R from $(P, -\epsilon, q)$ to $(P', -\epsilon', q')$.*

Proof. Obvious from Definition 1.8.

DEFINITION 4.3. If $\gamma = (P, \epsilon, q)$ is a form over R, we define γ^{op}, the opposite form to γ, to be the form $(P, -\epsilon, q)$. If Γ is a form-class over R, we define Γ^{op}, the opposite of Γ, to be the form-class $\{\gamma^{\mathrm{op}}: \gamma \in \Gamma\}$ over R.

LEMMA 4.18. *If γ is a form over R, and $f: R \to S$ is a ring-homomorphism, then $(\gamma_f)^{\mathrm{op}} = (\gamma^{\mathrm{op}})_f$.*

Proof. Obvious.

PROPOSITION 4.19. *If $\gamma = (P, \epsilon, q)$ is a form over R, then the form γ^{op} has the same discriminant, parity, and divisor as γ. If Γ is a form-class over R, Γ, and Γ^{op} have the same divisor and form-type.*

Proof. Reduce to the case where R is quasi-local and γ is associated with $[a, b, c]^L$ with respect to the properly oriented basis $\{e_1, e_2\}$; then $\gamma^{\mathrm{op}} = (P, -\epsilon, q)$ is associated with $[a, -b, c]^L$ with respect to the properly orientee basis $-\{e_1, e_2\}$ and we are done since the numerical forms $[a, b, c]^L$ and $[a, -b, c]^L$ over R clearly have the same discriminant, parity, and divisor over R.

We complete our proof that $PC_R(\tau)$ constitutes an Abelian group under composition, with a proof that every element has an inverse.

THEOREM 4.20. *Let $\gamma = (P, \epsilon, q)$ be a form over R of type $\tau = (\delta, \pi)$. If γ is primitive, then γ and γ^{op} are composable and $\gamma\gamma^{\mathrm{op}}$ is properly equivalent to $\iota(\tau)$. When γ is primitive, a proper equivalence.*

$$J_\gamma : P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}} \to R\tau$$

over R from $\gamma\gamma^{\mathrm{op}}$ to $\iota(\tau)$ is well-defined by the formula

$$J_\gamma(p_1 \otimes_{R\tau} p_2) = B_q(p_1 \otimes_R p_2) - \Phi_\epsilon(p_1 \otimes_R p_2)\langle\delta^{1/2}\rangle \tag{52}$$

(*cf. Definitions* 1.3, 1.8 *and Eq.* (8) *of Sect.* 3).

Remark. The above choice of J_γ was suggested by the composition identity

$$(ax_1^2 + bx_1x_2 + cx_2^2)(ay_1^2 + by_1y_2 + cy_2^2) = X_1^2 - bX_1X_2 + acX_2^2 \\ = N_m(X_1 + X_2\sigma_b)$$

with

$$X_1 = ax_1y_1 + bx_2y_1 + cx_2y_2\,, \\ X_2 = -x_1y_2 + x_2y_1\,,$$

and essentially involves a basis-free formulation of this identity; cf. formulas (65) and (66) in the proof below.

Proof of Theorem 4.20. In the first place, some special notation will be needed, to deal with the fact that an R-module structure and two $R\tau$-module structures (P_γ and $P_{\gamma^{\mathrm{op}}}$) are simultaneously being considered on P. During the course of this proof we shall write (for r in R, s in $R\tau$, p in P)

$$rp, \quad s \circ p, \quad s \circ\circ p$$

to denote the products associated, respectively, with the given R-module structure on P, the $R\tau$-module structure P_γ on P, and the $R\tau$-module structure $P_{\gamma^{\mathrm{op}}}$ on P.

Note that for r in R and p in P,

$$rp = r \circ p = r \circ\circ p.$$

Note also that the $R\tau$-module structure $P_{\gamma^{\mathrm{op}}}$ on P is the "conjugate" structure to P_γ, i.e., we have, for s in $R\tau$ and p in P,

$$s \circ\circ p = \bar{s} \circ p.$$

[To prove this, it suffices to show that, τ being $(\delta, b + 2R)$, we have $\sigma_b \circ\circ p = \bar{\sigma}_b \circ p$. Now (cf. Definition 1.7)

$$\Phi_{-\epsilon} = -\Phi_\epsilon\,, \qquad \lambda_{-\epsilon} = -\lambda_\epsilon$$

whence (cf. Eq. (14) of Proposition 3.2) $T(\gamma^{\mathrm{op}}) = -T(\gamma)$, so indeed

$$\sigma_b \circ\circ p = T_b(\gamma^{\mathrm{op}})p = \tfrac{1}{2}(T(\gamma^{\mathrm{op}})p - bp) = \tfrac{1}{2}(-T(\gamma)p - bp) \\ = -bp - \tfrac{1}{2}(T(\gamma)p - bp) = (-b - \sigma_b) \circ p = \bar{\sigma}_b \circ p.]$$

To prove Theorem 4.20 we must verify, in the given order, the four following statements:

(a) For all p_1 and p_2 in P,

$$B_q(p_1 \otimes_R p_2) - \Phi_\epsilon(p_1 \otimes_R p_2)\langle\delta^{1/2}\rangle$$

lies in $2(R\tau)$.

(b) The map

$$J'_\gamma : P_\gamma \times P_{\gamma^{\mathrm{op}}} \to R\tau,\ (p_1, p_2) \mapsto \tfrac{1}{2}(B_q(p_1 \otimes_R p_2) - \Phi_\epsilon(p_1 \otimes_R p_2)\langle\delta^{1/2}\rangle)$$

is $R\tau$-bilinear.

(c) The $R\tau$-homomorphism given by (52) is an $R\tau$-isomorphism.

(d) $((J_\gamma)^{-1})_*\iota(\tau)$ is a semi-composite of γ and γ^{op}.

Since γ and γ^{op} are primitive and of the same type by Proposition 4.19, it follows from Theorem 4.11 that they are composable. Thus, the proof of Theorem 4.20 will be complete once (a), (b), (c), and (d) are established.

It suffices to verify these four statements under the assumption that R is quasi-local, since $\iota(\tau)$, B_q, Φ_ϵ, $R\tau$, $\langle\delta^{1/2}\rangle$, P_γ, γ^{op}, $\gamma\gamma^{\mathrm{op}}$ and thus (once (a), (b), and (c) have been proved) J_γ and $(J_\gamma^{-1})_*(\iota(\tau))$ behave well under localization (cf. Lemmas 1.7, 1.8, 3.1, 3.3, and 4.18, and Theorems 4.1 and 4.7). Thus, *we assume for the remainder of this proof that P is free over R, and that γ is represented by $[a, b, c]^L$ with respect to the properly oriented free basis $\{e_1, e_2\}$ over R.*

It follows that $\tau = (b^2 - 4ac, b + 2R)$ and that

$$c(b) = ac, \qquad \sigma_b{}^2 + b\sigma_b + ac = 0. \tag{53}$$

Let

$$p_1 = x_1e_1 + x_2e_2, \qquad p_2 = y_1e_1 + y_2e_2 \tag{54}$$

with x_1, x_2, y_1, and y_2 in R; then $B_q(p_1 \otimes_R p_2) - \Phi_\epsilon(p_1 \otimes_R p_2)\langle\delta^{1/2}\rangle$ may readily be computed (using (2) and (31) of Section 1 and (8) of Section 3); it lies in $2R\tau$ (which proves (a)) and is twice the following expression:

$$J'_\gamma(p_1, p_2) = (ax_1y_1 + bx_2y_1 + cx_2y_2) + \sigma_b(x_2y_1 - x_1y_2). \tag{55}$$

To prove (b), it suffices to verify that

$$\sigma_b J'_\gamma(p_1, p_2) = J'_\gamma(\sigma_b \circ p_1, p_2) = J'_\gamma(p_1, \sigma_b \circ\circ p_2). \tag{56}$$

By Proposition 3.2, Corollary 1,

$$\sigma_b \circ p_1 = -(bx_1 + cx_2)e_1 + ax_1e_2, \tag{57}$$

$$\sigma_b \circ\circ p_2 = \bar{\sigma}_b \circ p_2 = (-b - \sigma_b) \circ p_2 = cy_2e_1 - (ay_1 + by_2)e_2. \tag{58}$$

Using these last two equations, together with (53) and (55), it is now straightforward to compute the three quantities in (56) and verify that they all equal

$$ac(x_1y_2 - x_2y_1) + \sigma_b(ax_1y_1 + bx_1y_2 + cx_2y_2),$$

which completes the proof of (b).

(a) and (b) together show there is an $R\tau$-homomorphism J_γ well defined by (52). We may now rewrite (55) as

$$J_\gamma(p_1 \otimes_{R\tau} p_2) = (ax_1y_1 + bx_2y_1 + cx_2y_2) + \sigma_b(x_2y_1 - x_1y_2). \tag{59}$$

We next turn to the proof of (c), i.e., the proof that

$$J_\gamma : P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}} \to R\tau$$

is bijective.

$P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$ is generated over R by the four elements

$$e_{ij} = e_i \otimes_{R\tau} e_j \qquad (i, j = 1 \text{ or } 2).$$

The identities

$$(\sigma_b \circ e_i) \otimes_{R\tau} e_j = e_i \otimes_{R\tau} (\sigma_b \circ\circ e_j) \qquad (i, j = 1 \text{ or } 2)$$

together with (57) and (58) yield the following relations over R on the e_{ij}:

$$ae_{12} + ae_{21} = be_{11}, \tag{60a}$$

$$ce_{11} = ae_{22}, \tag{60b}$$

$$ce_{12} + ce_{21} = be_{22}. \tag{60c}$$

(These generate all relations over R on the e_{ij}, but we do not need this fact.) We thus know the structure of $P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$ as an R-module; its additional structure as an $R\tau$-module may be specified, using

$$\sigma_b(e_i \otimes_{R\tau} e_j) = (\sigma_b \circ e_i) \otimes_{R\tau} e_j$$

and (57), by the equations

$$\sigma_b e_{11} = -be_{11} + ae_{21}, \tag{61a}$$

$$\sigma_b e_{12} = -be_{12} + ae_{22}, \tag{61b}$$

$$\sigma_b e_{21} = -ce_{11}, \tag{61c}$$

$$\sigma_b e_{22} = -ce_{12}. \tag{61d}$$

Finally, the action of J_γ may be specified in terms of this generating set $\{e_{ij}\}$; using (59), we obtain

$$J_\gamma e_{11} = 1, \quad J_\gamma e_{12} = -\sigma_b, \quad J_\gamma e_{21} = b + \sigma_b, \quad J_\gamma e_{22} = c. \tag{62}$$

Since, by hypothesis, γ is primitive, there exist a', b', and c' in R with

$$aa' + bb' + cc' = 1. \tag{63}$$

Let

$$\lambda = a'e_{11} + b'(e_{12} + e_{21}) + c'e_{22};$$

then it follows from (62) and (63) that $J_\gamma(\lambda) = 1$. Thus, an obvious candidate for an inverse map to J_γ is the $R\tau$-homomorphism

$$K\colon R\tau \to P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}},\ s \mapsto s\lambda$$

which maps 1 into λ. Clearly, $J_\gamma \circ K$ is the identity map on $R\tau$, and we shall now complete our proof that J_γ is an isomorphism by verifying that $K \circ J_\gamma$ is the identity map on $P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$.

Using (62) and (63) we see that

$$\begin{aligned} K(J_\gamma(e_{11})) - e_{11} &= K(a) - e_{11} = a\lambda - (aa' + bb' + cc')e_{11} \\ &= b'(ae_{12} + ae_{21} - be_{11}) + c'(ae_{22} - ce_{11}) \end{aligned}$$

which is 0 by (60a) and (60b). Similarly,

$$\begin{aligned} K(J_\gamma(e_{12})) - e_{12} &= -\sigma_b\lambda - e_{12} \\ &= [(ba' + cb')e_{11} + (bb' + cc')e_{12} - aa'e_{21} - ab'e_{22}] - (aa' + bb' + cc')e_{12} \\ &= a'(be_{11} - ae_{12} - ae_{21}) + b'(ce_{11} - ae_{22}) = 0. \end{aligned}$$

Two similar computations, which are here omitted, show that

$$(K \circ J)(e_{21}) = e_{21}, \qquad (K \circ J)(e_{22}) = e_{22}.$$

Since the e_{ij} generate $P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$ over R, it follows that $K \circ J_\gamma$ is the identity map, which completes the proof of (c). Note that we have also proved

$$(J_\gamma)^{-1} = K.$$

The proof of (d), and so of Theorem 4.20, will thus be complete if we prove that the form

$$\bar{\gamma} = (\bar{P}, \bar{\epsilon}, \bar{q}) = K_*(\iota(\tau)),$$

is a semi-composite of γ and γ^{op}; we shall do this by verifying conditions (i), (ii), and (iii) of Definition 4.1.

(Ad (i) The form-type of $K_*(\iota(\tau))$ is the same as that of $\iota(\tau)$, by Lemma 1.11, namely, τ; this is the form-type of γ and (by Proposition 4.19) of γ^{op}.

(Ad (ii) $\bar{P}$ denotes $K(R\tau) = P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$ considered as an R-module, and in the present case (ii) asserts that the $R\tau$-modules (each with $\bar{P}$ as underlying R-module) $\bar{P}_{\bar{\gamma}}$ and $P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$ coincide. This is an immediate consequence of the fact that the map $K\colon R\tau \to P$ is both an $R\tau$-isomorphism $R\tau \to \bar{P}_{\bar{\gamma}}$ (by Lemma 3.3(i)) and an $R\tau$-isomorphism $R\tau \to P_\gamma \otimes_{R\tau} P_{\gamma^{\mathrm{op}}}$ (as we saw in the proof of (c)).

(Ad (iii) We must show that for all p_1 and p_2 in P,

$$\bar{q}(p_1 \otimes_{R\tau} p_2) = q(p_1)\, q(p_2). \tag{64}$$

Now, $\bar{q} = ((J_\gamma)^{-1})_* N_m$, so $\bar{q}(p_1 \otimes_{R\tau} p_2) = N_m(J_\gamma(p_1 \otimes_{R\tau} p_2))$. This shows, using (62) together with Eq. (10) in Section 3, that (64) is equivalent to the composition identity

$$(ax_1^2 + bx_1x_2 + cx_2^2)(ay_1^2 + by_1y_2 + cy_2^2) = X_1^2 - bX_1X_2 + acX_2^2, \tag{65}$$

where

$$X_1 + X_2\sigma_b = J_\gamma((x_1e_1 + x_2e_2) \otimes_{R\tau} (y_1e_1 + y_2e_2)),$$

i.e., by (59),

$$\begin{aligned} X_1 &= ax_1y_1 + bx_2y_1 + cx_2y_2\,, \\ X_2 &= -x_1y_2 + x_2y_1\,. \end{aligned} \tag{66}$$

This compsition identity may be verified either by direct computation, or by appeal to Theorem 2.2, using the matrix

$$\Sigma = \begin{pmatrix} a, & 0, & b, & c \\ 0, & -1, & 1, & 0 \end{pmatrix}.$$

THEOREM 4.21. *Let R be a ring on which 2 is not a zero-divisor, and let $\tau = (\delta, \pi)$ be a form-type over R, i.e., an element of $R \times (R/2R)$ such that*

$$b \in \beta \Rightarrow b^2 \equiv \delta \pmod{4R}.$$

Then the collection $PC_R(\tau)$ (of all primitive form-classes over R of type τ) constitutes an Abelian group, under the restriction to this set of the operation "composition" given by Definition 4.2.

If, also, f is a ring-homomorphism from R to a ring S on which 2 is not a zero-divisor, then

$$PC_f(\tau)\colon PC_R(\tau) \to PC_S(\tau_f),\ \operatorname{cls}\gamma \mapsto \operatorname{cls}\gamma_f$$

is a group-homomorphism.

In the special case when $R = \mathbb{Z}$ and

$$\delta \equiv 0 \pmod 4,\quad \pi = 2\mathbb{Z}, \text{ or } \delta \equiv 1 \pmod 4,\quad \pi = 1 + 2\mathbb{Z}, \tag{67}$$

the group $PC_{\mathbb{Z}}(\tau)$ is isomorphic in a canonical fashion to the Gaussian group $G(\delta)$ defined by Theorem 2.3.

Remark. It also follows immediately from the preceding results that the class $PF_R(\tau)$ of all primitive forms of type τ over R, regarded as a category whose morphisms are the proper R-equivalences, together with the operation of composition given by Definition 4.1, is a "category with product" (i.e., composition of primitive forms is "coherently commutative and associative" in the sense of [29]; cf. also [00, Chap. VII]).

Proof. The first part of this theorem has already been proved; let us now summarize what has been done:

If γ and γ' are primitive forms over R of type τ, then they are composable by Theorem 4.11; their composite $\gamma\gamma'$ is of type τ by Definition 4.1(i), and is primitive since

$$\operatorname{div}(\gamma\gamma') = (\operatorname{div}\gamma)(\operatorname{div}\gamma') = RR = R$$

by Theorem 4.8. Passing to form-classes, by Definition 4.2, this shows that the composition of form-classes over R induces a binary operation on $PC_R(\tau)$. Compsition on $PC_R(\tau)$ is commutative by Theorem 4.13, and associative by Theorem 4.15. Next, Theorem 4.16 shows that cls $\iota(\tau)$ (cf. Definition 3.1) is the identity element in $PC_R(\tau)$. Finally, if Γ is any form-class in $PC_R(\tau)$, then the form-class Γ^{op} given by Definition 4.3 is also in $PC_R(\tau)$ by Proposition 4.19, and Theorem 4.20 shows that the composite $\Gamma\Gamma^{\mathrm{op}}$ is the identity element cls $\iota(\tau)$ of the composition group $PC_R(\tau)$.

The second assertion of the theorem, concerning the behavior of the composition groups under change of rings, follows immediately from Theorem 4.1.

Finally, suppose $R = \mathbb{Z}$. It is immediate from Definition 3.1 that the form-types $\tau = (\delta, \pi)$ over $\mathbb{Z}$ are given by (67), so that τ is uniquely determined by δ (cf. also the discussion of the Butts–Estes condition in Section 1, following the proof of Proposition 1.13. Here, δ can be any integer $\equiv 0$ or 1 (mod 4), and we write $PC_{\mathbb{Z}}(\delta)$ instead of $PC_{\mathbb{Z}}(\tau)$. As in Theorem 2.3, let us denote by $G(\delta)$ the set of all proper numerical binary Lagrangian quadratic form-classes over $\mathbb{Z}$. As observed in the discussion preceding Definition 1.10.

$$i\colon G(\delta) \to PC\mathrm{s}(\delta),\ \delta\mathrm{ls}[a, b, c]^L \to \delta\mathrm{ls}\left(R^2, \binom{1}{0} \wedge \binom{0}{1}, [a, b, c]^L\right)$$

whose image is the set of all $\gamma = (P, \epsilon, q)$ in $PC_{\mathbb{Z}}(\mathrm{B})$ for which P is free. Since every projective $\mathbb{Z}$-module is free, i is a bijection. To show i is an isomorphism, and so complete the proof of Theorem 4.21, it suffices to prove that if q, q', and Q are primitive numerical forms over $\mathbb{Z}$ of discriminant δ, and Q is the Gaussian composite of q and q', then $i(Q)$ is properly equivalent to the composite $i(q)\,i(q')$; this follows immediately from Theorem 4.5.

References

1. F. Arndt, *S.B. Akad. Wiss. Wien Math.* **31** (1858), 33–67.
2. H. Bass, "Algebraic K-Theory," Benjamin, New York, 1968.
3. H. Bass, Modules which support non-singular forms, *J. Algebra* **13** (1969), 246–252.
4. M. Bazin, Sur la théorie de la composition des formes quadratiques, *J. Math.* **16** (1851), 161–170.

5. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York/London, 1966.
6. N. Bourbaki, "Éléments de Mathématique," Livre II, Chap. I, Hermann, Paris, 1942.
7. Brahmegupta, "Brahme-sphut'a-sidd hanta," Chap. 18, Sect. 65–66 (translation by H. T. Colebrooke, 1817, under the title: "Algebra," with Arithmetic and Mensuration, "from the Sanscrit, of Brahmegupta and Bhascara"; cf. also discussion of this text in [II]).
8. H. S. Butts and B. J. Dulin, Composition of binary quadratic forms over integral domains, *Acta Arithmetica*, in press.
9. H. S. Butts and D. Estes, Modules and binary quadratic forms over integral domains, *Linear Algebra Appl.* 1 (1968), 153–180.
10. H. S. and G. Pall, Modules and binary quadratic forms, *Acta Arithmetica* **15** (1968), 23–44.
11. M. Chasles, Note sur les équations indéterminées du second degré, *J. Math.* **2** (1837), 37–50.
12. C. Chevalley, "Fundamental Concepts of Algebra," Academic Press, New York, 1956.
13. H. Cohn, "A Second Course in Number Theory," Wiley, New York/London, 1962.
14. L. E. Dickson, "Introduction to the Theory of Numbers," Dover, New York, 1957.
15. L. E. Dickson, "History of the Theory of Numbers," Vol. III, Chelsea, New York, 1952.
16. Diophantus of Alexandria, "Arithmetika"](Sir T. L. Heath, Transl.), Dover, New York, 1964.
17. G. L. Dirichlet, De formarum binariarum secundi gradus compositione, *J. Math.* **47** (1854), 155–160.
18. G. L. Dirichlet, "Vorlesungen über Zahlentheorie," 2nd ed., with "Supplements" added by R. Dedekind, Vieweg und Sohn, Braunschweig, 1871.
19. L. Euler, "Corresp. Math. Phys." (Fuss, Ed.), Vol. I, pp. 616–617, 629–631, 1843; letters to Goldbach, Aug. 4, 1753 and Aug. 23, 1755."
20. L. Euler, "Vollständige Anleitung zur Algebra," Kays. Acad. der Wissenschaften, 1770; "Opera Omnia," Series Prima, Volumen Primum, (Theil 2, Abschnitt 2, Capitel 11, §178), Teubner, Leipzig/Berlin, 1911.
21. H. Flanders, On free exterior powers, *Trans. Amer. Math. Soc.* **145** (1969), 357–367.
22. C. F. Gauss, "Disquisitiones Arithmeticae," Fleischer, Leipzig, 1801; English transl. by A. A. Clarke, S. J., Yale Univ. Press, New Haven, Conn., London, 1966.
23. J. H. Grace and A. Young, "The Algebra of Invariants," Cambridge Univ. Press, Cambridge, 1903.
24. A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique, I, *Publ. Math. Inst. Hautes Études Sci.*, N0. 4 (1960).
25. I. Kaplansky, Composition of binary quadratic forms, *Studia Math.* **5** (1968), 523–530.
26. J. L. Lagrange, "Œuvres," Gauthier–Villars, Paris, 1867-1892.
27. Legendre, "Essai sur la théorie des nombres", Chez Duprat, Paris, 1798.
28. S. Lubelski, Unpublished results on number theory, II (posthumous; edited by C. Schogt), *Acta Arithmetica* **7** (1961/1962), 9–17.
29. S. MacLane, Natural associativity and commutativity, *Rice Univ. Studies* **49** (1963), 28–46.
30. T. Muir, "A Treatise on the Theory of Determinants" (revised by W. H. Metzler), Dover, New York, 1960.

31. J. H. S. SMITH, "Collected Mathematical Papers," Oxford Univ. Press (Clarendon), Oxford, 1894.
32. A. SPEISER, "Festschrift H. Weber," pp. 375–395, Teubner, Leipzig/Berlin, 1912.
33. J. TOWBER, Complete reducibility in exterior algebras over free modules, *J. Algebra* **10** (1968), 299–309.